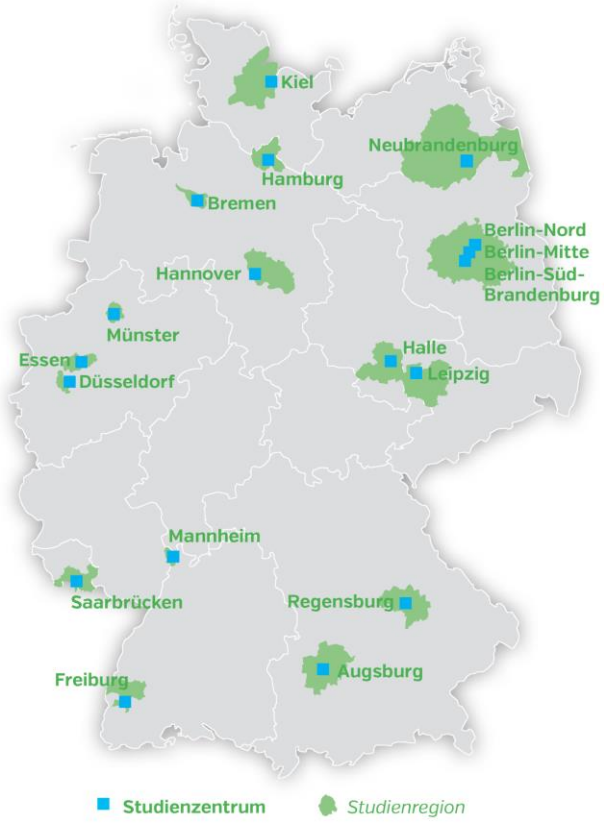
Gemeinsam forschen für eine gesündere Zukunft

Datenschutz- und IT-Sicherheitskonzept des Kompetenzzentrums Mortalitäts-Follow-Up der NAKO Gesundheitsstudie

http://www.nako.de/



Version 2.0, Stand: 05.06.2018

Gefördert vom Bund,
den Ländern und der
Helmholtz-Gemeinschaft

Vorbemerkung:

Mit der Bezeichnung „Teilnehmer“ sind stets sowohl Männer als auch Frauen gemeint. Lediglich aufgrund der Lesbarkeit und Textlänge wird auf die Nennung der weiblichen Formen verzichtet.

Datenschutzrechtlich verantwortlich:

NAKO e.V.

c/o Geschäftsstelle
Am Taubenfeld 21/2
69123 Heidelberg
Tel.: 06221/ 42-620-0
Fax: 06221/ 42-620-99

E-Mail: geschaeftsstelle@nako.de
http://www.nako.de/

Herausgeber und operativ verantwortlich:

Kompetenzzentrum Mortalitäts-Follow-Up der NAKO Gesundheitsstudie

Bundesinstitut für Bevölkerungsforschung
Friedrich-Ebert-Allee 4
65185 Wiesbaden

Tel.: +49-611-75-4173
Fax: +49-611-75-3960

E-Mail: NAKO@bib.bund.de
http://www.bib-demografie.de/

Inhalt

1 Einleitung 5
1.1 Das Kompetenzzentrum Mortalitäts-Follow-Up der NAKO 5
1.2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten 5
1.2.1 Bundesdatenschutzgesetz und sonstige gesetzliche Datenschutzbestimmungen 6
1.2.2 EU Datenschutz-Grundverordnung 6

1.2.3 Bundesmeldegesetz ... 6
1.2.4 Personenstandsgesetz ... 7
1.2.5 Bestattungsrecht der Bundesländer ... 7
1.2.6 Ärztliche und andere Berufsordnungen ... 8
1.2.7 Ethikkommissionen – gesetzliche Basis und Satzungen ... 8
1.2.8 Auskünfte durch Angehörige ... 9
1.2.9 Normen des BSI zur IT-Sicherheit ... 9
2 Grundsätze des Datenschutzes des Kompetenzzentrums ... 10
2.1 Verantwortliche Stelle ... 10
2.2 Zweck der Datenverarbeitung ... 10
2.3 Arten personenbezogener Daten ... 11
2.4 Datenspeicherung ... 11
2.5 Maßnahmen zum Datenschutz ... 12
3 Strukturen des Mortalitäts-Follow-Ups ... 13
3.1 Kompetenzzentrum Mortalitäts-Follow-Up ... 13
3.2 Meldebehörden ... 13
3.3 Meldeauskunft-Dienstleister ... 13
3.4 Gesundheitsämter ... 14
3.5 Standesämter ... 14
4 Prozesse der Datenverarbeitung ... 16
4.1 Vitalstatusermittlung ... 16
4.1.1 Vorbedingungen ... 16
4.1.2 Beteiligte Einrichtungen ... 16
4.1.3 Ablauf ... 16
4.2 Todesursachenermittlung ... 19
4.2.1 Vorbedingungen ... 19
4.2.2 Beteiligte Einrichtungen ... 20
4.2.3 Ablauf ... 20
5 Organisatorische Maßnahmen ... 26
5.1 Mitarbeiter ... 26
5.2 Räumlichkeiten ... 26
6 Technische Maßnahmen: datenverarbeitende Anlage ... 27
6.1 IT-Netzwerk ... 27
6.2 VPN-Verbindungen ... 29
6.3 SINA-Workstations ... 29
6.4 Drucker und Scanner ... 30
6.5 Schriftgut mit IDAT und MDAT (MoFU-Daten) ... 30
6.6 Betriebssystem des MoFU-Servers ... 31

6.7 Anwendersoftware 31
6.8 Datenaustauschformat 32
7 Technische Maßnahmen: Prozesse der Datenverarbeitung 33
7.1 Datenübertragung 33
7.2 Datensicherung 33
8 Technische Maßnahmen: Dokumentation 34
9 Abkürzungsverzeichnis 35
10 Anhang 36
11 Separate Anlagen 37
11.1 Synopse: Rechtliche Regelungen des Zugangs wissenschaftlicher Forschung zur Todesbescheinigung nach Bundesländern 37
11.2 Beispiel: Bayerische Todesbescheinigung 37
11.3 Bevollmächtigungen des Meldeauskunft-Dienstleisters durch das Bundesinstitut für Bevölkerungsforschung 37
11.4 Anschreiben an die Gesundheitsämter zur Anforderung der Todesbescheinigungen 37
11.5 Anschreiben an die Ärzte und Krankenhäuser zur Anforderung von Todesursachen .....**Fehler! Textmarke nicht definiert.**

1 Einleitung

Das vorliegende Konzept beschreibt alle Maßnahmen zum Datenschutz und zur IT-Sicherheit für das Kompetenzzentrum Mortalitäts-Follow-Up („Mortalitäts-Follow-Up“) der NAKO Gesundheitsstudie.

1.1 Das Kompetenzzentrum Mortalitäts-Follow-Up der NAKO

Das Kompetenzzentrum Mortalitäts-Follow-Up der NAKO ist eine zentrale Einrichtung der NAKO Gesundheitsstudie und wird vom Bund, den Ländern und der Helmholtz-Gemeinschaft gefördert (Förderkennzeichen 01ER1511D). Es ist am Bundesinstitut für Bevölkerungsforschung in Wiesbaden, einer Ressortforschungseinrichtung im Geschäftsbereich des Bundesministeriums des Inneren, angesiedelt.

Das Mortalitäts-Follow-Up hat im Einzelnen die Aufgaben,

1. die regelmäßige Feststellung des Vitalstatus aller Teilnehmer der NAKO – die aktuelle Adresse oder bei Verstorbenen diese Tatsache und Sterbeort, Sterbedatum und gegebenenfalls auch den Staat des Sterbeortes;
2. die Erhebung der Todesursachen verstorbener Teilnehmer aus den Todesbescheinigungen bei den Gesundheitsämtern und aus weiteren Quellen und die Codierung dieser nach der Diagnosen Klassifikation (International Classification of Diseases and Related Health Problems „ICD“) der Weltgesundheitsorganisation („WHO“) in der aktuellen Version (gegenwärtig Version 10);

Die vom Kompetenzzentrum Mortalitäts-Follow-Up erhobenen Daten sind von entscheidender Bedeutung für den Zweck der NAKO Gesundheitsstudie: die Bestimmung gesundheitsfördernder und gesundheitsschädlicher Einflüsse in der Allgemeinbevölkerung.

1.2 Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Die vom Mortalitäts-Follow-Up verarbeiteten Daten sind alle einer bestimmten oder bestimmbaren, von der NAKO Gesundheitsstudie untersuchten Person (Teilnehmer) zugeordneten Gesundheitsdaten und sonstigen besonderen und anderen Daten, die das Mortalitäts-Follow-Up der NAKO Gesundheitsstudie im Rahmen seiner Aufgaben erhebt, nutzt, verarbeitet oder mit der Unabhängigen Treuhandstelle (THS), mit dem Integrationszentrum (IntZ), mit dem Meldeauskunft-Dienstleister und Registern, mit Ärzten, Gesundheitseinrichtungen oder anderen Stellen austauscht.

Wesentlich sind dabei Daten, die aus

1. der Ermittlung des Vitalstatus,
2. der Ermittlung der in der amtlichen Todesbescheinigung dokumentierten Todesursachen verstorbener Teilnehmer und sonstigen Mortalitätsinformationen über sie,
3. der Ermittlung von zusätzlichen Informationen über Todesursachen und sonstige Umstände des Todes bei behandelnden Ärzten, anderen Versorgungsleistern und unter besonderen Umständen Angehörigen des Verstorbenen – etwa bei Versterben im Ausland, oder Versterben durch Unfall außerhalb des Wohnorts, wenn die Todesbescheinigung durch einen Arzt, der den Teilnehmer nicht kannte, unzureichende Informatio-

nen über Nebendiagnosen oder eventuelle Grundleiden wie Diabetes, Epilepsie, chronischer Tablettenmissbrauch enthält.

stammen.

Von herausgehobener Bedeutung sind damit folgende Rechtsgrundlagen:

1.2.1 Bundesdatenschutzgesetz und sonstige gesetzliche Datenschutzbestimmungen

Das Bundesdatenschutzgesetz (BDSG) gilt für das Mortalitäts-Follow-Up sowohl wegen der Beauftragung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit („BfDI“) durch nach § 5 der Bund-Länder Vereinbarung vom 29. Juni 2012 (BAnzAT 12.04.2013 B5) als auch wegen der Tatsache, dass das Mortalitäts-Follow-Up seine Aufgaben an einem Bundesinstitut erfüllt.

Die für das Mortalitäts-Follow-Up relevanten Vorschriften des BDSG sind die auch für andere datenverarbeitende Einrichtungen innerhalb der NAKO Gesundheitsstudie bedeutsamen und deshalb auch im Allgemeinen Datenschutz- und IT-Sicherheitskonzept der NAKO Gesundheitsstudie erwähnt.

Der Datenschutz, der aufgrund gesetzlicher Melde- und Auskunftspflichten erhobenen Daten für die Erhebung (1) des Vitalstatus, (2) der Todesursachen und sonstigen Mortalitätsinformationen auf den Todesbescheinigungen, wird im Bundesmeldegesetz, Personenstandsgesetz und –verordnung, sowie in den Bestattungsgesetzen und –verordnungen der Länder geregelt.

Zum Schutz der vom Mortalitäts-Follow-Up zusätzlich erhobenen Daten über Todesursachen und sonstige Umstände des Todes bei behandelnden Ärzten, anderen Versorgungsleistern und ggf. Angehörigen des Verstorbenen ist zusätzlich das Berufsrecht der Ärzte, der Psychotherapeuten und gegebenenfalls anderer Gesundheitsberufe heranzuziehen.

1.2.2 EU Datenschutz-Grundverordnung

In der EU-Datenschutz-Grundverordnung 2016/679 vom 27.04.2016 ist relevant folgende Vorschrift:

„Gründe

(27) Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen“. Siehe auch die Zitierung dieser Vorschrift in den Gründen (158) und (160).

Die Verordnung ist seit 25.05.2016 in Kraft, gilt ab 25.05.2018, prägt bereits die Datenschutzgesetzgebung in den Mitgliedstaaten.

1.2.3 Bundesmeldegesetz

Im Bundesmeldegesetz (BMG) ist relevant § 44 „*Einfache Melderegisterauskunft*“, wonach auch ohne Zustimmung des Betroffenen Auskunft über Familienname, Vornamen, Doktorgrad, derzeitige Anschriften sowie, sofern die Person verstorben ist, diese Tatsache von der Meldebehörde (siehe Abschnitte 3.2 und 3.3) auf Verlangen mitgeteilt werden können, sofern diese Daten nicht für Werbung oder Adresshandel verwendet werden.

Bei Teilnehmern, die nicht im Bereich des für ihren Wohnort zuständigen Gesundheitsamts versterben, ist relevant § 45 (1) 9 „*Erweiterte Melderegisterauskunft*“. Danach kann bei Verstorbenen auch Auskunft über das Sterbedatum, den Sterbeort sowie bei Versterben im Ausland auch den Staat, gegeben werden, soweit ein berechtigtes Interesse glaubhaft gemacht wird.

Absatz (2) Halbsatz 1, wonach die Meldebehörde die betroffene Person über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten hat, ist offensichtlich hier nicht anwendbar.

1.2.4 Personenstandsgesetz

Das Personenstandgesetz (PStG) gewährt in § 66 ein Forschungsprivileg, das vom Mortalitäts-Follow-Up bei fehlerhaften Melde- oder Studiendaten, sowie für weitere Zwecke in Einzelfällen möglicherweise beansprucht werden muss: Danach kann Hochschulen und anderen Einrichtungen, die wissenschaftliche Forschung betreiben, Auskunft aus einem oder Einsicht in ein Personenstandsregister sowie Durchsicht von Personenstandsregistern gewährt werden, wenn dies für die Durchführung bestimmter wissenschaftlicher Forschungsvorhaben erforderlich ist, eine Nutzung anonymisierter Daten zu diesem Zweck nicht möglich oder die Anonymisierung mit einem unverhältnismäßigen Aufwand verbunden ist und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen an dem Ausschluss der Benutzung erheblich überwiegt.

Voraussetzung sind ausreichende technische und organisatorische Maßnahmen zum Datenschutz bei der Verarbeitung der so übermittelten Daten. Die Genehmigung der obersten Landesbehörde muss eingeholt werden.

1.2.5 Bestattungsrecht der Bundesländer

Die Bestattungs- oder Friedhofsgesetze der Bundesländer oder die zugehörigen Verordnungen sind relevant, weil sie die Ermittlung der Todesursachen durch den leichenschauenden Arzt, ihre Dokumentation in der Todesbescheinigung, deren Verbleib in den Gesundheitsämtern (siehe Abschnitt 3.4) und den Zugang zu diesen Informationen für die wissenschaftliche Forschung regeln.

Stellvertretend wird aus § 9 (7) des Gesetzes über das Friedhofs- und Bestattungswesen des bevölkerungsreichsten Bundeslandes Nordrhein-Westfalen (Stand 09.07.2014) zitiert:

Danach kann die untere Gesundheitsbehörde auf Antrag im erforderlichen Umfang Auskünfte aus der Todesbescheinigung erteilen, Einsicht gewähren oder Ablichtungen davon aushändigen, wenn u.a.

„ … die antragstellende Person die Angaben für ein wissenschaftliches Forschungsvorhaben benötigt und

a) die verstorbene oder die bestattungspflichtige Person der Datenverarbeitung zugestimmt hat und durch unverzügliche Anonymisierung oder Pseudonymisierung der Angaben sichergestellt wird, dass schutzwürdige Belange der oder des Verstorbenen und der Angehörigen nicht beeinträchtigt werden,

oder

b) das Ministerium festgestellt hat, dass das öffentliche Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse der oder des Verstorbenen und der Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Sobald der Forschungszweck es gestattet, sind die Daten der oder des Verstorbenen so zu verändern, dass ein Bezug zur Person nicht mehr erkennbar ist."

Ähnliche Regelungen in teilweise identischer Formulierung gibt es in der Mehrzahl der Bundesländer. Auch wo es solche Regelungen nicht gibt, wird anscheinend gleich verfahren.

Das Mortalitäts-Follow-Up hält eine Synopse über die einschlägigen bestattungsrechtlichen Regelungen auf jeweils neuestem Stand, die diesem Konzept als Anhang beigefügt ist.

1.2.6 Ärztliche und andere Berufsordnungen

Die Gesetze der Bundesländer über die Heilberufe beauftragen die Kammern solcher Berufsgruppen, Berufsordnungen zu erlassen, die nach behördlicher Genehmigung für die betreffenden Berufsgruppen Gesetzeskraft haben.

Relevant ist § 9 in der Formulierung der ärztlichen Muster-Berufsordnung, die freilich erst in Gestalt der Berufsordnungen der jeweiligen Landeärztekammern Gesetzeskraft erhält. Sachverhalte, die der in Absatz (1) beschriebenen Schweigepflicht auch über den Tod des Patienten hinaus unterliegen, zu offenbaren, ist Ärztinnen und Ärzten nach (2) erlaubt, sofern sie von der Schweigepflicht wirksam (§ 4a BDSG) entbunden wurden. Da solche Auskünfte gegenüber der NAKO Gesundheitsstudie, sofern diese zusätzliche Mortalitätsinformationen erheben will, nicht im Behandlungsvertrag der Teilnehmer mit ihren behandelnden Ärzten vorgesehen sein dürften, sind solche Auskünfte jedoch stets freiwillig, müssen dann aber wahrheitsgetreu sein. Das ärztliche Schweigegebot ist nach § 203 StGB strafbewehrt.

Analoges gilt für andere Gesundheitsberufe, die verstorbene Teilnehmer zu Lebzeiten selbständig behandelt hatten (z.B. Schweigegebot § 11 der Muster Berufsordnung Psychologischer Psychotherapeuten; Verschwiegenheitspflicht nach § 7 der zahnärztlichen Muster Berufsordnung).

Sind Angehörige der genannten Gesundheitsberufe an der Forschungstätigkeit im Kompetenzzentrum beteiligt, so haben sie die datenschutzrechtliche Verschwiegenheitspflicht auch als persönliche Berufspflicht zu beachten. Da Teilnehmer der NAKO Studie wirksame Einwilligungserklärungen abgegeben haben, gilt das Schweigegebot nicht innerhalb der Studie, sofern dies dem Studienzweck zuwiderlaufen würde. Eine Weitergabe von IDAT und MDAT (MoFU-Daten) an Dritte wäre bei Angehörigen der genannten Gesundheitsberufe auch ein Verstoß gegen berufsrechtliche Pflichten.

1.2.7 Ethikkommissionen – gesetzliche Basis und Satzungen

Grundsätzlich gilt nach § 5 der Bund-Länder Vereinbarung über die NAKO vom 29. Juni 2012 (BAnzAT 12.04.2013 B5) die Pflicht aller Teilprojekte der NAKO, sich bei den örtlich zuständigen Ethikkommissionen beraten zu lassen. Ethikkommissionen werden nach Landesrecht an den Hochschulen und den Landesärztekammern gebildet. In den Satzungen der Ethikkommissionen ist die Möglichkeit der Übernahme der Voten anderer Ethikkommissionen vorgesehen, wovon bei multizentrischen Studien mit einer federführenden Ethikkommission – für die

NAKO ist dies die Ethikkommission der Bayerischen Landeärztekammer – regelmässig Gebrauch gemacht wird.

Sind Angehörige der genannten Gesundheitsberufe an der Forschungstätigkeit im Kompetenzzentrum beteiligt, so haben sie sich als persönliche Berufspflicht über die berufsrechtlichen und berufsethischen Fragen bei der für sie zuständigen Ethikkommission beraten zu lassen, da bei dieser Forschungstätigkeit *„Körpermaterialien oder Daten verarbeitet werden, die sich einem bestimmten Menschen zuordnen lassen“* (§ 15 (1) in der Formulierung der ärztlichen Musterberufsordnung, analog § 11 der Muster Berufsordnung Psychologischer Psychotherapeuten). Diese persönliche Berufspflicht gilt unabhängig von der in der Bund-Länder Vereinbarung festgehaltenen Beratungspflicht durch die jeweils zuständigen Ethikkommissionen.

Voten der Ethikkommission sind für Angehörige der genannten Heilberufe auch für die Durchführung von Vorhaben der Beobachtungsepidemiologie verbindlich.

1.2.8 Auskünfte durch Angehörige

Angehörige von Teilnehmern unterliegen im Allgemeinen keinen Schweigepflichten. Sie können nicht durch irgendwelche Willenserklärungen der Teilnehmer zu Lebzeiten gegenüber der NAKO zu Auskünften nach deren Tod verpflichtet werden. Auskünfte von Angehörigen, sofern sie als Daten verstorbenen Teilnehmern zuzuordnen sind, unterliegen wie alle anderen Daten strengen Datenschutztauflagen und werden streng vertraulich behandelt.

1.2.9 Normen des BSI zur IT-Sicherheit

Für den Betrieb und damit die Sicherheit der datenverarbeitenden Anlagen des Mortalitäts-Follow-Up ist das ITZBund, der IT-Dienstleister des Bundes (https://www.itzbund.de) verantwortlich. Neben den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik kommen bei der Tätigkeit des ITZBund auch interne Regelwerke zur Anwendung, die im Allgemeinen jedoch nicht öffentlich zugänglich sind.

2 Grundsätze des Datenschutzes des Kompetenzzentrums

2.1 Verantwortliche Stelle

Das Mortalitäts-Follow-Up verantwortet die Erfüllung der in 1.1 beschriebenen Aufgaben im Rahmen des Vertrages zur Datenverarbeitung im Auftrag nach § 11 BSG und seiner Anlagen, des Studienprotokolls, der Vorhabenbeschreibung, und des vorliegenden Dokuments einschließlich der zugehörigen SOPs, im Rahmen der Weisungen des Vorstands des Nationale Kohorte e.V. als Projektleiter der NAKO Gesundheitsstudie und Auftraggeber des Vertrags zur Datenverarbeitung im Auftrag.

Das Bundesinstitut für Bevölkerungsforschung verantwortet die allgemeine Ausstattung und den sicheren Betrieb der IT-Infrastruktur, wobei es sich der Dienste des ITZBund bedient, und im Rahmen einer Verwaltungsgemeinschaft bestimmte Verwaltungsaufgaben durch das Statistischen Bundesamt wahrgenommen werden.

2.2 Zweck der Datenverarbeitung

Das Mortalitäts-Follow-Up hat im Einzelnen die Aufgaben,

1. den Vitalstatus aller Teilnehmer - die aktuelle Adresse oder bei Verstorbenen diese Tatsache und Sterbeort, Sterbedatum und gegebenenfalls auch den Staat des Sterbeortes - festzustellen und an die Unabhängige Treuhandstelle zu übermitteln, mit denen seit mehr als 6 Monaten kein Kontakt durch das rekrutierende Studienzentrum bestand;
2. die Todesursachen verstorbener Teilnehmer aus den Todesbescheinigungen bei den Gesundheitsämtern zu erheben und nach der aktuellen Diagnosen Klassifikation (International Classification of Diseases and Related Health Problems „ICD“) der Weltgesundheitsorganisation („WHO“) zu codieren;
3. pseudonymisierte, digitalisierte Kopien der Todesbescheinigungen zu erstellen;
4. unvollständige oder fehlerhafte Angaben auf den Todesbescheinigungen durch Befragung der behandelnden Ärzte, anderer Versorgungsleistern und Hinterbliebener zu verbessern und zu ergänzen, und dann ebenfalls zu codieren und weiterzugeben;
5. die Todesursachencodes aus beiden Quellen zusammen mit den Kopien der Todesbescheinigungen und einem Protokoll über Zusatzerhebungen pseudonymisiert an das Integrationszentrum zu übermitteln;
6. an qualitätssichernden Maßnahmen der NAKO Gesundheitsstudie teilzunehmen;

Zweck dieser Datenverarbeitung ist die Erhebung der allgemeinen Sterblichkeit – damit der unterschiedlichen Lebensdauer – und der Todesursachen unter den Teilnehmern der NAKO Gesundheitsstudie. Diese Informationen sind für den Zweck der NAKO Gesundheitsstudie, nämlich der Bestimmung gesundheitsfördernder und gesundheitsschädlicher Einflüsse in der Allgemeinbevölkerung von entscheidender Bedeutung. Siehe auch Abschnitt 1.1.

2.3 Arten personenbezogener Daten

Das Mortalitäts-Follow-Up verarbeitet personenbezogene Daten, d.h. bestimmten oder bestimmbaren, von der NAKO Gesundheitsstudie untersuchten Personen (Teilnehmer) zugeordnete Daten (MoFU-Daten) von zwei Arten:

- IDAT sind personenidentifizierende Daten, die das Mortalitäts-Follow-Up mit der THS, mit Meldeauskunft-Dienstleistern und Melderegistern und in Einzelfällen auch mit Personenstandsregistern austauscht.
- MDAT sind Daten über die Todesursachen und über weitere Todesumstände, die das Mortalitäts-Follow-Up nach abgeschlossener qualitätsgeprüfter Erhebung an das Integrationszentrum (IntZ) übermittelt.

Eine Doppelrolle spielen Daten zum Sterbedatum und Sterbeort (ggfs. mit Angabe des Staates), die sowohl zur Identifikation von Personen, wie zur Gesundheitsmessung - Lebensdauer, saisonale und regionale Einflüsse auf das Sterberisiko und das Todesursachenprofil, unterschiedliche Codierpraxis in unterschiedlichen Ländern – verwendet werden können.

Rechtsgrundlagen sind beschrieben in Abschnitt 1.2.

2.4 Datenspeicherung

IDAT und MDAT (MoFU-Daten) werden grundsätzlich nur kurzfristig gespeichert und nur soweit dies erforderlich ist für die Aufgaben der Datenerhebung, Qualitätskontrolle und sicheren Datenübermittlung an die THS und an das IntZ. Für die Vitalstatuserhebung beträgt die Speicherfrist grundsätzlich 12 Monate und für die Todesursachenerhebung grundsätzlich 24 Monate.

Von außen empfangenes Schriftgut auf Papier (Todesbescheinigungen, Obduktionsbefunde, Briefe und ähnliches) mit personenbezogenen Daten der Teilnehmer der NAKO Studie wird sofort nach dem Eingang in abschließbaren sicheren Schränken im MoFU-Arbeitsraum aufbewahrt, bis die auf ihnen vorhandenen Daten entweder in vorgesehener Weise in die entsprechende Datenbank eingepflegt oder nach unumkehrbarer Entfernung der personenidentifizierenden Daten pseudonymisiert, digitalisiert und gespeichert wurden.

Die Daten und die pseudonymisierten digitalisierten Kopien des Schriftgutes werden an die THS oder das IntZ versandt.

Nach erfolgtem Versand der Daten oder der pseudonymisierten digitalisierten Kopien an die THS oder das IntZ und Erhalt der jeweiligen Empfangsbestätigung wird das zugrundeliegende Schriftgut im MoFU unverzüglich, frühestens aber nach Ablauf von 24 Stunden nach der Speicherung der auf dem Schriftgut vorhandenen Daten vernichtet (siehe auch Abschnitte 4.2.3 (13) und 6.6 (2).

Bei der Vitalstatuserhebung speichert das Mortalitäts-Follow-Up alle zu diesem Vorgang zugehörigen IDAT – den von der THS erhaltenen Datensatz und den an die THS übermittelten Teildatensatz – bis nach der Übertragungsbestätigung der THS. Sodann löscht das Mortalitäts-Follow-Up alle zu diesem Vorgang zugehörigen IDAT. Der Löschvorgang wird mit einem Löschprotokoll im MoFU dokumentiert (siehe Abschnitte 4.1.3 (13) und (15)).

Bei der Todesursachenermittlung speichert das Mortalitäts-Follow-Up alle zu diesem Vorgang zugehörigen personenbezogenen Daten – den von der THS erhaltenen Datensatz und den an

die THS und an das IntZ übermittelten Teildatensatz – bis nach den Übertragungsbestätigungen der THS und des IntZ. Sodann löscht das Mortalitäts-Follow-Up den von der THS erhaltenen Datensatz, die an das IntZ und die THS übermittelten Datensätze und alle damit im Zusammenhang stehenden personenbezogenen Daten (inkl. aller Kopien der Todesbescheinigungen und der Protokoll der Todesursachenermittlungen) (siehe Abschnitte 4.2.3 (25)) unverzüglich, frühestens aber nach Ablauf von 24 Stunden.

Eine regelmäßige Datensicherung erfolgt auf einem Backup-Server (beschrieben in Abschnitten 6 und 7). Die Aufbewahrungsfrist für diese Datensicherungen beträgt maximal 24 Monate. (siehe Abschnitt 7.2 (4)).

2.5 Maßnahmen zum Datenschutz

Die Mitarbeiter des Mortalitäts-Follow-Up werden vor der Aufnahme ihrer Tätigkeit auf das Datengeheimnis nach § 5 BDSG verpflichtet.

Die Aufgaben als behördlicher Beauftragter für den Datenschutz werden beim Bundesinstitut für Bevölkerungsforschung von dem Datenschutzbeauftragten des Statistischen Bundesamtes wahrgenommen. Stellt der Datenschutzbeauftragte bzw. die Institution selbst in diesem Zusammenhang Unregelmäßigkeiten fest, wird unverzüglich der NAKO e.V. informiert.

Auch alle anderen für Datensicherheit und Datenschutz zuständigen Abteilungen des Statistischen Bundesamtes stehen dem Mortalitäts-Follow-Up beratend zur Verfügung.

Die IT-Infrastruktur – Hard- und Software – wird vom ITZBund (https://www.itzbund.de) betrieben.

Einzelheiten des rechtlichen und technischen Datenschutzes sind im Vertrag zur Datenverarbeitung im Auftrag zwischen dem NAKO e.V. als Auftraggeber und dem Bundesinstitut für Bevölkerungsforschung als Auftragnehmer dokumentiert und geregelt.

3 Strukturen des Mortalitäts-Follow-Ups

3.1 Kompetenzzentrum Mortalitäts-Follow-Up

Das Kompetenzzentrum Mortalitäts-Follow-Up besteht gegenwärtig aus einem Team von drei Wissenschaftlern und einer Projektadministration. Das Team wird finanziert von der NAKO Gesundheitsstudie. Träger und Projektnehmer ist das Bundesinstitut für Bevölkerungsforschung in der Friedrich-Ebert-Allee 4, 65185 Wiesbaden. Das Bundesinstitut für Bevölkerungsforschung besteht in einer Verwaltungsgemeinschaft mit dem Statistischen Bundesamt.

Das Mortalitäts-Follow-Up hat verschiedene, im folgenden Text und in den Schematischen Darstellungen 1 und 2 genauer beschriebene technische Schnittstellen zu anderen NAKO Einrichtungen: zur Unabhängigen Treuhandstelle und zum Integrationszentrum, daneben bestehen Schnittstellen zu einem externen Meldeauskunft-Dienstleister.

Zu Studienzentren, zu Ärzten in Zusammenhang mit dem Versterben des Teilnehmers, sonstigen Versorgungseinrichtungen in Zusammenhang mit dem Versterben des Teilnehmers oder Angehörigen verstorbener Teilnehmer und zu lokalen Melderegistern und zu Gesundheitsämtern, in Einzelfällen auch zu Standesämtern, wenn eine gesuchte Vitalstatusinformation nur dort zu finden ist, werden telefonische oder briefliche Kontakte je nach Stand der Aufgabenerfüllung aufgebaut.

Weitere Informationen zu den Mitarbeitern und Räumlichkeiten werden in Abschnitt 5 dargestellt, zur IT-Architektur in Abschnitt 6.

3.2 Meldebehörden

Aufgrund des Bundesmeldegesetzes sind die Länder verpflichtet Meldebehörden (siehe Abschnitt 1.2.3) einzurichten, die dieses Gesetz anzuwenden haben. Im Regelfall sind sie auf kommunaler Ebene eingerichtet, ihre IT-Struktur und Datensätze sind zunehmend auch auf Landesebene oder darüber hinaus zusammengefasst.

Das Mortalitäts-Follow-Up benötigt Zugang zu den Registern der Meldebehörden, um für die Erhebung des Vitalstatus von Teilnehmern (siehe Abschnitt 4.1) die aktuelle Adresse oder bei Verstorbenen diese Tatsache sowie Sterbeort, Sterbedatum und gegebenenfalls auch den Staat des Sterbeortes in Kenntnis zu bringen.

Im Regelfall bedient sich das Mortalitäts-Follow-Up bei diesem Zugang der Dienste von Meldeauskunft-Dienstleistern (siehe Abschnitt 3.3), wird aber in unklaren Einzelfällen selbst an Meldebehörden zur Gewinnung der gesuchten Mortalitätsinformationen herantreten.

3.3 Meldeauskunft-Dienstleister

Die Erhebungen des Vitalstatus im Mortalitäts-Follow-Up werden grundsätzlich in den Melderegistern der nach Landesrecht zuständigen Meldebehörden durchgeführt. Die kommunal organisierten Meldebehörden haben ihre Melderegister im Verlauf der letzten Jahre bundeslandesweit, teilweise über Bundeslandgrenzen hinweg vernetzt, wobei unterschiedliche technische Lösungen verwirklicht wurden. Die Nutzung solcher Netze, die für Melderegisterauskünfte erheblich Kosten und Zeit einspart, bieten kommerzielle Meldeauskunft-

Dienstleister, zunehmend auch kommunale Portale, im Rahmen eines Vertrags zur Datenverarbeitung im Auftrag an.

Die Nutzung solcher Dienstleister ist für die Erhebungen des Vitalstatus im Mortalitäts-Follow-Up von zentraler Bedeutung.

Nach erfolgter Ausschreibung entsprechend der gesetzlichen Regelungen für Bundeseinrichtungen schloss das Bundesinstitut als Auftragnehmer und mit Zustimmung des Nationale Kohorte e.V. als Auftraggeber einen weiteren Vertrag zur Datenverarbeitung im Auftrag nach § 11 BDSG mit einem Unterauftragnehmer ab, dem Meldeauskunft-Dienstleister:

RISER ID Services GmbH (https://www.riserID.eu)
Charlottenstraße 80
10117 Berlin.

Gegenstand des Vertrags ist die Auskunft über die aktuelle Adresse von Teilnehmern (siehe 4.1.3). Die Firma wurde gegenüber Dritten entsprechend bevollmächtigt (siehe Anlage 11.3).

Der Dienstleister hat bekannte Referenzen aus dem Bereich der wissenschaftlichen epidemiologischen Forschung und ist von der datenschutz cert GmbH (https://www.datenschutz-cert.de) - ein Unternehmen der datenschutz nord Gruppe - und von der EuroPrise Gmbh (https://www.european-privacy-seal.eu) zertifiziert.

Weitere Verträge mit Meldeauskunft-Dienstleistern sind zur Erfüllung der Aufgaben des Mortalitäts-Follow-Ups geplant.

3.4 Gesundheitsämter

Gesundheitsämter sind Einrichtungen der Landkreise / kreisfreien Städte mit hoheitlichen und nicht-hoheitlichen Aufgaben im Bereich der Prävention, Diagnostik, Therapie von Krankheiten und anderen Gesundheitsstörungen. Sie unterstehen der Fachaufsicht des jeweiligen für den Öffentlichen Gesundheitsdienst zuständigen Landesministeriums.

Die Anwendung der Bestimmungen der Bestattungsgesetze (siehe Abschnitt 1.2.5) über die Todesursachendiagnosen und Dokumentation in den Todesbescheinigungen ist hoheitliche Aufgabe. Überwiegend werden die Todesursachendiagnosen von den leichenschauenden Ärzten auf Papierformularen dokumentiert, die mit einer Registriernummer („Sterbebuchnummer“) im Original im Gesundheitsamt verbleiben. Ein Durchschlag ohne Name und Adresse des Verstorbenen geht an das Statistische Landesamt.

Das Mortalitäts-Follow-Up benötigt Zugang zu den Todesursachendiagnosen und sonstigen Mortalitätsinformationen in den Todesbescheinigungen verstorbener Teilnehmer der NAKO Gesundheitsstudie. Dieser Zugang ist zentral für die Aufgabenerfüllung des Mortalitäts-Follow-Up.

3.5 Standesämter

Aufgrund des Personenstandsgesetzes (PStG) des Bundes, sind die Länder verpflichtet Standesämter einzurichten (siehe Abschnitt 1.2.4).

Das Mortalitäts-Follow-Up wird in Einzelfällen auch an Standesämter herantreten zwecks Zugangs zu Sterberegistern, aber auch zu anderen Registern. Beispielsweise kann § 27 (4) PStG, wonach im Geburtenregister auf den Tod des Kindes, eine das Kind betreffende Todes-

erklärung oder gerichtliche Feststellung der Todeszeit hingewiesen wird, bei anderweitig fehlenden Daten einer von der NAKO Gesundheitsstudie untersuchten Person einen eigenen Weg zum zuständigen Gesundheitsamt und der Todesbescheinigung eröffnen.

4 Prozesse der Datenverarbeitung

4.1 Vitalstatusermittlung

4.1.1 Vorbedingungen

1) Die Vitalstatuserhebung ermittelt bei Teilnehmern nach §44 des Bundesmeldegesetzes (BMG), ob sie noch unter der bisherigen Wohnadresse (Hauptwohnung), als verzogen nach einer neuen Wohnadresse, als unbekannt verzogen, oder als „Verstorben“ gemeldet sind. Bei Verstorbenen werden nach §45 BMG das Sterbedatum und der Sterbeort (bei Versterben im Ausland auch der Staat) ermittelt. Das Einholen dieser Auskünfte bei den Meldebehörden (siehe Abschnitte 1.2.3 und 3.2) ist nicht einwilligungspflichtig. Diese Vitalstatuserhebung wird nicht für Teilnehmer durchgeführt, die ihre Einwilligungserklärung vollständig widerrufen haben.
2) Die Vitalstatusermittlung wird vom Mortalitäts-Follow-Up durchgeführt, um verstorbene Teilnehmer zu identifizieren. Als Nebeneffekt werden die Datenbanken der Unabhängigen Treuhandstelle und darüber des Teilnehmermanagements der Studienzentren mit den aktuellen Adressen nicht-verstorbener Teilnehmer aktualisiert.
3) Insoweit das Bundesinstitut für Bevölkerungsforschung zur Vitalstatuserhebung einen Meldeauskunft-Dienstleister nutzt, wird mit diesem einen Vertrag nach § 11 BDSG zur Datenverarbeitung im Auftrag geschlossen mit genauen Vorgaben zur Datenverarbeitung (siehe Abschnitt 3.3).

4.1.2 Beteiligte Einrichtungen

Beteiligte Einrichtungen sind neben dem Mortalitäts-Follow-Up, die Unabhängige Treuhandstelle (THS), Meldeauskunft-Dienstleister, Meldebehörden, in Ausnahmefällen Studienzentren (SZ), Standesämter. Zu jeder Datenübertragung von und zu einer dieser Einrichtungen, und jeder Speicherung der übertragenen Daten wird eine Vorgangsnummer vergeben.

4.1.3 Ablauf

1) Das MoFU erfragt etwa zweimonatlich über das Portal der THS, bei welchen Teilnehmern in den 6 Monaten zuvor kein Kontakt stattgefunden hat.
2) Die THS erzeugt für jeden dieser Teilnehmer jeweils ein eindeutiges Pseudonym ID-V als Zufallszahl und speichert dessen Zuordnung zum Teilnehmer.
3) Die THS stellt für diese Teilnehmer einen Datensatz (Datensatz I) mit Vorgangsnummer und Zeitstempel zusammen, in dem für jeden Teilnehmer die folgenden personenidentifizierenden Daten (IDAT) enthalten sind:
    1) Pseudonym ID-V,
    2) Nachname,
    3) Vornamen,
    4) Geschlecht,

5) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
6) derzeitige Staatsangehörigkeiten,
7) letzte bekannte Wohnadresse (Hauptwohnung).

4) Das Mortalitäts-Follow-Up ruft im Portal der THS diese nach aktuellem Pretty Good Privacy (PGP) Standard verschlüsselt bereitgestellten Daten über VPN ab (siehe Abschnitt 7.1). Das Mortalitäts-Follow-Up nimmt den Datensatz (Datensatz I) in Empfang, prüft diesen auf Vollständigkeit und Konsistenz. Der Eingang des Datensatzes (Datensatz I) wird mit einem Eingangsprotokoll mit den Informationen Vorgangsnummer, Eingangsdatum, Größe des Datensatzes festgehalten.

5) Das Mortalitäts-Follow-Up übermittelt die unter Nummer (3) aufgeführten Informationen (Datensatz II) zeitnah - allerdings ohne das Pseudonym ID-V - an den externen Meldeauskunft-Dienstleister zur Überprüfung des Vitalstatus. Ein temporäres Pseudonym (ID-ADL) wird vom MoFU für jeden Teilnehmer vergeben, dessen Daten übermittelt werden. Die Datenübergabe an den Meldeauskunft-Dienstleister erfolgt über VPN, ebenfalls verschlüsselt über aktuelles PGP Verfahren als VSC-Datei (pro Individuum eine Zeile) mit den folgenden Informationen:

1) ID-ADL,
2) Nachname,
3) Vornamen,
4) Geschlecht,
5) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
6) derzeitige Staatsangehörigkeiten,
7) letzte bekannte Wohnadresse (Hauptwohnung).

6) Der Meldeauskunft-Dienstleister führt Melderegisterabfrage (Melderegisterauskunftsabfrage für Datensatz II) durch und übermittelt als Ergebnis die Melderegisterauskunft (Meldeauskunft für Datensatz II) dem Mortalitäts-Follow-Up die Ergebnisse der Vitalstatusermittlung (Datensatz III).

7) Das Mortalitäts-Follow-Up kontrolliert die übermittelten Ergebnisse auf Vollständigkeit, Plausibilität und sonstige Qualitätsmerkmale.

8) Das Mortalitäts-Follow-Up aktualisiert den von der THS erhaltenen Datensatz (siehe Schritt 3) aufgrund der Ergebnisse. Neben diesen geänderten Daten (z.B. Änderung von Namen oder Staatsangehörigkeiten, Korrektur der Geburtsangaben) werden zusätzlich folgende Informationen aus der aktuellen einfachen Melderegisterauskunft nach(§44 BMG) erfasst:

   Auskunftsstatus:

   - „Adresse aktiv“;
   - „verzogen nach“ (bisherige Adresse wird überschrieben);
   - „unbekannt verzogen“ (Adressfeld bleibt leer);
   - „verstorben“;

9) Bei verstorbenen Teilnehmern wird zusätzlich im Wege der erweiterten Melderegisterauskunft (§45 BMG) Sterbedatum, Sterbeort, bei Versterben im Ausland auch der Staat erhoben.

10) Für Teilnehmer, für die vom Meldeauskunft-Dienstleister keine valide einfache oder erweiterte Melderegisterauskunft erhalten wurden, wird das Mortalitäts-Follow-Up den Vitalstatus nach vorheriger Abstimmung mit den Studienzentren in Einzelabfragen über die zuständigen lokalen Melderegister (und ggf. andere öffentliche Register – etwa Personenstandsregister) oder, falls so keine Anschrift ermittelt werden kann, auch anderweitig prüfen (weitere Meldeauskunftsabfrage für Datensatz II).

11) Das Mortalitäts-Follow-Up erstellt mit diesen Informationen einen Datensatz (Datensatz IV) und übermittelt diesen mit der von der THS verwendeten Vorgangsnummer und verschlüsselt nach aktuellem PGP Standard über VPN an die THS mit folgenden Informationen:

    1) Pseudonym ID-V,
    2) Nachname,
    3) Vornamen,
    4) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
    5) Geschlecht,
    6) derzeitige Staatsangehörigkeiten,
    7) aktualisierte Adresse der Hauptwohnung,
    8) ggf. Sterbedatum,
    9) ggf. Sterbeort, sowie bei Tod im Ausland auch den Staat.

12) Die THS prüft die erhaltenen Daten auf Integrität und speichert diese in der eigenen Datenbank.

13) Die THS bestätigt dem Mortalitäts-Follow-Up die erfolgreiche Übertragung und Speicherung unter Angabe der Vorgangsnummer.

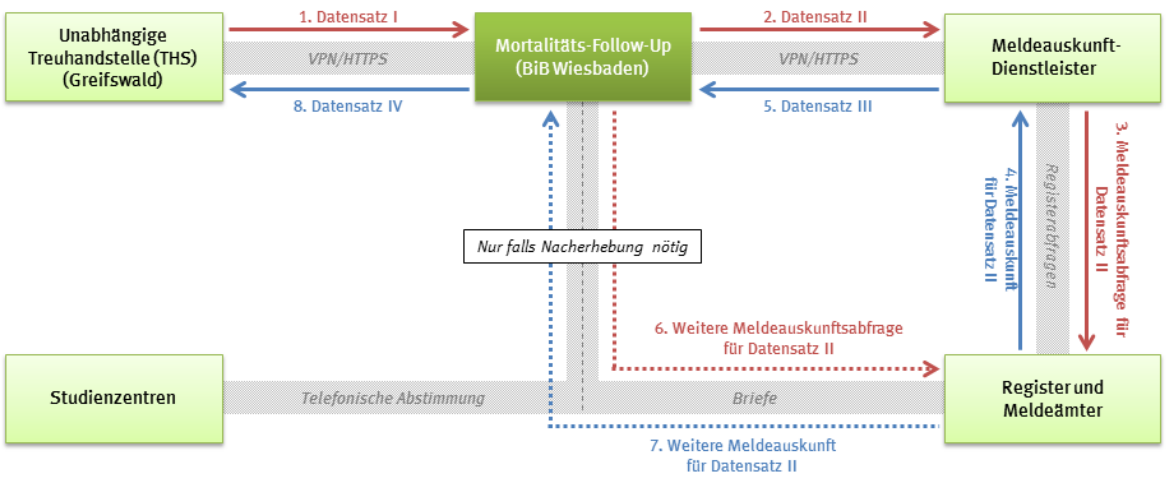
14) Das Mortalitäts-Follow-Up löscht nach der Übertragungsbestätigung der THS alle zu diesem Vorgang zugehörigen personenbezogenen Daten – den von der THS erhaltenen Datensatz und den an die THS übermittelten. Der Löschvorgang wird mit einem Löschprotokoll dokumentiert.

15) Die THS ermittelt die Teilnehmernummer für die erhaltenen ID-V und speichert die geänderten und ergänzten personenidentifizierenden Daten im Stammdatensatz der Teilnehmer.

16) Die THS synchronisiert die geänderten personenidentifizierenden Daten automatisch mit der Teilnehmerverwaltungssoftware MODYS in den Teilnehmermanagements der Studienzentren der NAKO Gesundheitsstudie.

Die Schematische Darstellung 1 „Vitalstatuserhebung“ zeigt die beschriebenen Zusammenhänge.

Vitalstatuserhebung



Schematische Darstellung 1: „Vitalstatuserhebung“ (verkürzt)

4.2 Todesursachenermittlung

4.2.1 Vorbedingungen

1. Das Ziel der Todesursachenermittlung ist, die Diagnosen für das Grundleiden und die einzelnen Schritte der Kausalkette bis zur unmittelbaren Todesursache, sowie eventuelle Nebendiagnosen bei jedem verstorbenen Teilnehmer durch Einsicht in die bei den Gesundheitsämtern aufbewahrten Todesbescheinigungen festzustellen, die in diesen dokumentierten Todesursachen nach der aktuellen Diagnosen Klassifikation (International Classification of Diseases and Related Health Problems „ICD“) der Weltgesundheitsorganisation („WHO“) zu codieren und an das Integrationszentrum zu übermitteln. Zusätzlich wird die genaue Todeszeit in Stunden und Minuten, die äußeren Umstände (Zuhause, im Pflegeheim, im Krankenhaus, auf der Straße usw.) des Sterbens, bestehende Schwangerschaft, Unfallgeschehen, Obduktionsbefund, u.a. ermittelt (siehe die Bayerische Todesbescheinigung in Anhang 11.2).
2. Bei den Teilnehmern, die entsprechende Einwilligungen unterzeichnet haben, werden zusätzlich zu diesen Informationen aus den Todesbescheinigungen entsprechende Informationen bei den behandelnden Ärzten, sonstigen Versorgungseinrichtungen, und in besonderen Ausnahmen bei Angehörigen verstorbener Teilnehmer erhoben.
3. Zur Einsichtnahme in die Todesbescheinigungen (siehe Abschnitte 1.1, 2.2, 2.3) bei den Gesundheitsämtern (siehe Abschnitt 3.4) besteht eine Rechtsgrundlage im Bestattungsrecht aller Länder (siehe Abschnitt 1.2.5 und die als Anlage 11.1 beige-

fügte Synopse: „Rechtliche Regelungen des Zugangs wissenschaftlicher Forschung zur Todesbescheinigung nach Bundesländern“. Kann eine Einwilligung des Teilnehmers zu Lebzeiten im Original oder als amtlich beglaubigte Kopie dem Gesundheitsamt vorgelegt werden, ist der Zugang problemlos. Kann eine solche Einwilligung nicht vorgelegt werden, bedarf der Zugang zu den nicht-anonymisierten Todesbescheinigungen einer Erlaubnis der obersten Landesbehörde, die dazu den Landesdatenschutzbeauftragten anzuhören hat. Die Erlaubnis darf nur erteilt werden, wenn der Forschungszweck nur durch Überlassung identifizierter Todesbescheinigungen erreicht werden kann, und das öffentliche Interesse an der Forschung gegenüber den schutzwürdigen Interessen des Verstorbenen und der Hinterbliebenen überwiegt.[1] Für den Mortalitäts-Follow-Up der Nako Gesundheitsstudie bedeutet das, dass wo immer möglich, eine solche Erlaubnis durch die für die Gesundheitsämter zuständige oberste Landesbehörde eingeholt werden soll. Andernfalls soll der Zugang zu den nicht-anonymisierten Todesbescheinigungen von verstorbenen NaKo Studienteilnehmern durch Vorlage der Einwilligungserklärung des Teilnehmers zu Lebzeiten in der vom Gesundheitsamt verlangten Form erreicht werden.

4. Für die Kontaktierung der behandelnden Ärzte muss der Teilnehmer zu Lebzeiten der Einwilligung „Ärzte, Gesundheitsämter und Angehörige im Todesfall“ zugestimmt haben. Die Teilnehmer entbinden mit der Einwilligung, sofern diese eine wirksame Schweigepflichtentbindung ist, die Ärzte für den in der Einwilligung Zweck von ihren Verschwiegenheitspflichten.

4.2.2 Beteiligte Einrichtungen

Beteiligte Einrichtungen sind neben dem Mortalitäts-Follow-Up die Unabhängige Treuhandstelle (THS), die Studienzentren (SZ), das Integrationszentrum (IntZ), die zuständigen Gesundheitsämter, die behandelnden Ärzte, sonstige Versorgungseinrichtungen (Pflegeheime, Hospize u.a.) und – als Kontaktstellen – Angehörige verstorbener Teilnehmer. Zu jeder Datenübertragung von und zu einer dieser Einrichtungen, und jeder Speicherung der übertragenen Daten vergibt das Mortalitäts-Follow-Up eine Vorgangsnummer.

4.2.3 Ablauf

1) Das MoFU erfragt etwa monatlich über das Portal der THS, welche die Teilnehmer innerhalb dieses Zeitraums als verstorben bekannt wurden, und für die noch keine Todesursachen ermittelt wurden.

2) Die THS erzeugt für jeden dieser Teilnehmer ein eindeutiges Pseudonym ID-TU als Zufallszahl und speichert dessen Zuordnung zum Teilnehmer.

[1] Diese Rechtslage hat sich auch durch die EU-Datenschutz-Grundverordnung vom 27. April 2016, die am 25.05.2018 in Kraft treten wird, nicht geändert. Dort steht in Grund 27 „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

3) Die THS stellt für diese Teilnehmer einen Datensatz (Datensatz A) zusammen, in dem für jeden Teilnehmer die folgenden personenidentifizierenden Daten (IDAT) enthalten sind:

    1) Pseudonym ID-TU
    2) Nachname
    3) Vornamen
    4) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch der Staat
    5) Geschlecht
    6) Staatsangehörigkeiten zum Zeitpunkt des Todes
    7) Sterbedatum, Sterbeort, sowie bei Tod im Ausland auch den Staat
    8) die Adresse der letzten Hauptwohnung

4) Die THS erzeugt eine eindeutige Vorgangsnummer. Das Mortalitäts-Follow-Up ruft bei der THS diese nach aktuellem Pretty Good Privacy (PGP) Standard verschlüsselt bereitgestellten Daten (Datensatz A) über VPN ab (siehe Abschnitt 7.1).

5) Das Mortalitäts-Follow-Up ermittelt die für die Sterbeorte zuständigen Gesundheitsämter.

6) Das Mortalitäts-Follow-Up übermittelt brieflich die Teildatensätze (Sterbefälle aus Datensatz A) an die jeweils zuständigen Gesundheitsämter zum Zweck der Einsichtnahme in die Todesbescheinigung. An die Gesundheitsämter werden dieselben Daten mit Ausnahme des Pseudonyms ID-TU übermittelt. Der Datensatz enthält dabei folgende Informationen:

    1) Nachname,
    2) Vornamen,
    3) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
    4) Geschlecht,
    5) Staatsangehörigkeiten zum Zeitpunkt des Todes,
    6) Sterbedatum, Sterbeort, sowie bei Tod im Ausland auch den Staat,
    7) Adresse der letzten Hauptwohnung.

7) Die Gesundheitsämter übermitteln dem Mortalitäts-Follow-Up eine Fotokopie der Todesbescheinigung (Todesbescheinigung aus Datensatz A) der Teilnehmer. Die Übersendung erfolgt brieflich.

8) Sollte dieser Kommunikationsweg nicht erfolgreich sein, muss eine eigenhändige Ablichtung oder Abschrift der Todesbescheinigung vor Ort im Gesundheitsamt durch die Mitarbeiter des Mortalitäts-Follow-Up erfolgen. Es besteht die Möglichkeit von telefonischen Nachfragen.

9) Das Mortalitäts-Follow-Up prüft die in der Todesbescheinigung – Vertraulicher Teil – enthaltenen Todesursachendiagnosen auf Vollständigkeit, Genauigkeit und Plausibilität.

10) Das Mortalitäts-Follow-Up dokumentiert Zusatzinformationen (Obduktionsschein, Unfall, bestehende Schwangerschaft u.a.) zum Sterbeort und anderen Mortalitätsinformationen.

11) Falls seit der letzten Untersuchung in einem Studienzentrum mehr als 12 Monate bis zum Tod vergangen sind, und von der Teilnehmerin oder dem Teilnehmer die entsprechende Einwilligung (4.4) gegeben wurde, führt das Mortalitäts-Follow-Up eine Nacherhebung zu den Todesursachen durch. Dies geschieht durch (a) Aufforderung an die THS, ID-P des Teilnehmers zusammen mit dem Kontaktwunsch an das Studienzentrum zu senden. Das Mortalitäts-Follow-Up erhält die ID-P nicht. Dann (b) nimmt das Mortalitäts-Follow-Up mit den Studienzentren Kontakt auf zwecks Befragungen bei Ärzten, anderen Versorgungsleistern und ggf. Angehörigen des Verstorbenen (Ermittlung der Zusatzinformationen der Todesursachen aus Datensatz A). Grundsätzlich kontaktiert das Mortalitäts-Follow-Up in solchen Fällen Ärzte, andere Versorgungsdienstleister und ggf. Angehörige der Verstorbenen nur, wenn Teilnehmer vor ihrem Tod aus der Rekrutierungsregion ihrer Studienzentren weggezogen waren, außerhalb der Rekrutierungsregion verstorben sind, oder das Studienzentrum selbst zu solchen Kontakten sich nicht in der Lage sieht.

    Leitlinie der Zusatzerhebung ist eine Auswahl der Fragen aus dem für weltweiten Einsatz konzipierte „Verbal Autopsy Instrument“ der Weltgesundheitsorganisation[2] zur Todesursachendiagnose durch Befragung in der aktuellen Version (2016, nächste Revision geplant für 2020). Eine autorisierte deutsche Fassung liegt nicht vor. Die ausgewählten Fragen werden von den MoFU-Mitarbeitern nach üblichen Regeln übersetzt werden.

    Es ist davon auszugehen, dass eine Kontaktaufnahme zu Angehörigen nur in äußerst seltenen Fällen notwendig sein wird. Die Kontaktaufnahme findet in der Regel durch das Studienzentrum statt bzw. nur nach vorheriger Kontaktierung des Studienzentrums und dessen ausdrücklicher Zustimmung zu einer Kontaktaufnahme durch das MoFU. Lediglich wenn der Teilnehmer außerhalb der Rekrutierungsregion verstorben ist, könnte das MoFU direkt den Kontakt aufnehmen. In der Regel wird dies jedoch auch nach vorheriger Abstimmung mit dem Studienzentrum geschehen. Erfragt werden sollen Informationen zu Todesumständen, Todesursachen und damit in Zusammenhang stehenden Vorerkrankungen.

12) Über die Durchführung und die Ergebnisse der Nacherhebung (Zusatzinformationen der Todesursachen aus Datensatz A) fertigt das Mortalitäts-Follow-Up ein elektronisches Protokoll an, ausschließlich mit der ID-TU und ohne den Namen des Verstorbenen.

13) Das Mortalitäts-Follow-Up digitalisiert und pseudonymisiert die Kopie der Todesbescheinigung durch eine unumkehrbare Entfernung der personenidentifizierenden Daten und eine Markierung mit dem Pseudonym ID-TU. Zur sicheren vorübergehenden Aufbewahrung der eingegangenen nicht-bearbeiteten Todesbescheinigungen und Papierdokumente (z.B. Obduktionsbefunde) ist ein verschließbarer Stahlschrank im MoFU-Arbeitsraum vorhanden. Die Papierdokumente, werden dort ebenfalls aufbewahrt, bis sie, nach unumkehrbarer Entfernung der personenidentifizierenden Daten, pseudonymisiert, digitalisiert und sicher gespeichert wurden. Die Dokumente werden

[2] http://www.who.int/entity/healthinfo/statistics/WHO_VA_2016_Manual_and_Questionnaires.zip

danach umgehend, frühestens aber nach Ablauf von 24 Stunden nach der Speicherung vernichtet.

14) Das Mortalitäts-Follow-Up prüft die Todesursachen für das Grundleiden, die Kausalkette bis zur unmittelbaren Todesursache, die Nebendiagnosen auf Vollständigkeit, Genauigkeit und Plausibilität.

15) Das Mortalitäts-Follow-Up codiert die Todesursachen in zwei Versionen:

I. Unter Verwendung ausschließlich der auf der Todesbescheinigung aufgeführten Diagnosen;
II. Unter Verwendung der auf der Todesbescheinigung aufgeführten Diagnosen zusammen mit allen zusätzlich nacherhobenen Informationen zu den Todesursachen aus dem Protokoll.

Hinweis: Die Codierung unter Verwendung ausschließlich der auf der Todesbescheinigung aufgeführten Diagnosen enthält weniger Informationen, ist aber erforderlich zum Vergleich des Todesursachenprofils der NAKO-Teilnehmer mit dem der Gesamtbevölkerung.

16) Codiert wird grundsätzlich mit Hilfe der der international eingeführten automatischen Codierungssoftware IRIS des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDI). Manuelle Nachcodierung ist in einer Minderzahl der Fälle erforderlich.

17) Das Mortalitäts-Follow-Up erstellt mit diesen Informationen zwei Datensätze (Datensatz B und Datensatz C), welche getrennt gespeichert bzw. getrennt an die beteiligten Einrichtungen nach 2.2.2. übermittelt werden:

18) Der erste Datensatz (Datensatz B) enthält folgende Informationen (IDAT):

1) Pseudonym ID-TU;
2) Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat;
3) Geschlecht;
4) Sterbedatum Sterbeort, Institutionenkennzeichen nach §293 SGB V, ARGE-IK-Verfahren sowie bei Tod im Ausland auch der Staat;
5) Staatsangehörigkeiten zum Zeitpunkt des Todes;
6) Adresse der letzten Hauptwohnung.

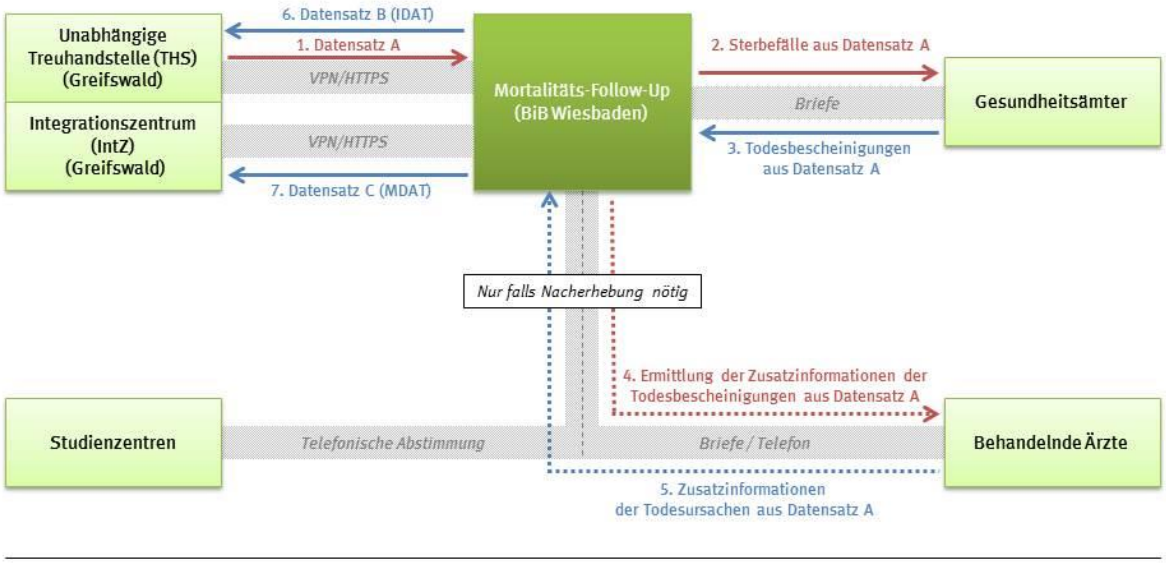
19) Die Datenübermittlung dieses Datensatzes erfolgt auf gleiche Weise wie bei der Vitalstatuserhebung an die THS, verschlüsselt über VPN nach aktuellem PGP Standard (siehe Abschnitt 4.1.3 (10)).

20) Der zweite Datensatz (Datensatz C) enthält folgende Informationen (MDAT):

1) Pseudonym ID-TU;
2) Sterbezeitpunkt in Stunden und Minuten (ist nur auf der Todesbescheinigung enthalten);
3) Todesursachendiagnosen Version I (nur aus den Daten der Todesbescheinigung);
4) Todesursachendiagnosen Version II (aus den Daten der Todesbescheinigung und der zusätzlich nacherhobenen Mortalitätsinformationen).

21) Das Mortalitäts-Follow-Up übermittelt einmalig und vollständig mit einer einmalig verwendeten Vorgangsnummer und verschlüsselt nach aktuellem PGP Standard über VPN an das IntZ:
    1) den beschriebenen zweiten Datensatz mit den ermittelten Todesursachen;
    2) die pseudonymisierte digitalisierte Todesbescheinigung;
    3) das Protokoll der Todesursachenermittlung II mitsamt der Nacherhebung der Zusatzinformationen.
22) Das IntZ prüft die erhaltenen Daten auf Integrität und speichert diese in einem geschützten, logisch abgetrennten Bereich der Studiendatenbank.
23) Die THS bestätigt dem Mortalitäts-Follow-Up die erfolgreiche Übertragung und Speicherung unter Angabe der Vorgangsnummer.
24) Das IntZ bestätigt dem Mortalitäts-Follow-Up die erfolgreiche Übertragung und Speicherung unter Angabe der Vorgangsnummer.
25) Das Mortalitäts-Follow-Up löscht den von der THS erhaltenen Datensatz, den an das IntZ und die THS übermittelten Datensatz und alle damit im Zusammenhang stehenden personenbezogenen Daten (inkl. aller Kopien der Todesbescheinigungen und der Protokoll der Todesursachenermittlungen.
26) Das IntZ speichert den Datensatz C (unter Umpseudonymisierung der ID-TU zur ID-F) mit den ermittelten Todesursachen in der Forschungsdatenbank der NAKO Gesundheitsstudie. Zugang zu diesen Daten zur wissenschaftlichen Nutzung kann fortan über die Transferstelle beantragt werden.

Die Schematische Darstellung 2 „Todesursachenermittlung“ zeigt verkürzt die beschriebenen Zusammenhänge.



Schematische Darstellung 2: „Todesursachenermittlung“ (verkürzt)

5 Organisatorische Maßnahmen

5.1 Mitarbeiter

1) Die MoFU-Mitarbeiter, die Zugang zu den IDAT und MDAT (MoFU-Daten) erhalten, sind lokal dokumentiert.

2) Die MoFU-Mitarbeiter und Administratoren sind auf das Datengeheimnis nach § 5 BDSG verpflichtet.

3) Personal des ITZBund oder Dritte erhält zu keinem Zeitpunkt Zugriff auf unverschlüsselte IDAT und MDAT (MoFU-Daten), mit der folgenden Ausnahme: Bei einer anderweitig nicht abwendbaren Gefahr eines endgültigen Datenverlustes, einer schwerwiegenden Beschädigung der Datenbank, oder anderen vergleichbaren Gefahren für den Zweck des Mortalitäts-Follow-Up, die die MoFU-Mitarbeiter nicht selbst abwenden können, eröffnen die MoFU-Mitarbeiter den namentlich benannten Administratoren den Zugang zu IDAT und MDAT (MoFU-Daten), soweit dies zur Abwendung der Gefahr erforderlich ist. Über solche Vorfälle wird von den MoFU-Mitarbeitern ein Protokoll erstellt, das den lokalen Datenschutzbeauftragten und dem Vorstand der NAKO zur Verfügung gestellt wird.

5.2 Räumlichkeiten

1) Die Verarbeitung der IDAT und MDAT (MoFU-Daten) findet statt:

   a. in zutrittsgesicherten, vom ITZBund genutzten Räumlichkeiten des Statistischen Bundesamtes am Standort Wiesbaden, in denen die Server stehen (siehe 6.2). Der Zutritt ist nur dem ITZBund-Personal möglich.

   b. im zutrittsgesicherten MoFU-Arbeitsraum des BIB, in dem alle Datenendgeräte stehen (siehe 6.4 – 6.6). Der Zutritt ist grundsätzlich nur den MoFU-Mitarbeitern möglich. Die individuelle Zutrittskontrolle der MoFU-Mitarbeiter erfolgt über ein elektronisches Schließsystem mittels einer maschinenlesbaren Zutrittskarte.

2) Der Zutritt zum MoFU-Arbeitsraum durch andere Personen einschließlich des IT- und des Reinigungspersonals ist nur im Beisein eines MoFU-Mitarbeiters möglich. Gesetzliche Zutrittsrechte (Gefahrenabwehr, Strafverfolgung u.a.) bleiben unberührt. Der Zutritt ist in einem Gästebuch mit Zeitangaben zu dokumentieren.

3) Der Transport von IDAT und MDAT (MoFU-Daten) ist außerhalb des MoFU-Arbeitsraums nur als Schriftgut auf Papierdatenträgern (Briefe) und möglichst nur durch MoFU-Mitarbeiter statthaft.

6 Technische Maßnahmen: datenverarbeitende Anlage

6.1 IT-Netzwerk

1) Die Verarbeitung der IDAT und MDAT (MoFU-Daten) und der Betrieb aller anderen beteiligten Dienste erfolgt nur auf über das Projekt beschaffter Hardware in einem abgeschotteten MoFU-Netzwerk im BiB und in den Rechenzentren des ITZBund am Standort Wiesbaden. Dabei wird der BSI-Grundschutz-Maßnahmenkatalog „M 5.117 Integration eines Datenbank-Servers in ein Sicherheitsgateway“ umgesetzt (zu den Räumlichkeiten siehe Abschnitt 5.2 (1)).

2) Das separierte MoFU-Netzwerk umfasst zwei Applikationsserver, zwei Datenbank-Server und einen Back-Up Server. Diese fünf Server befinden sich innerhalb des geschützten MoFU-Netzwerks und sind von allen anderen Netzwerken abgeschottet. Sie sind physisch aufgeteilt in zwei verschiedenen Brandabschnitten in den Räumlichkeiten des Statistischen Bundesamtes am Standort Wiesbaden (Rechenzentren betrieben durch ITZBund). Ein Applikationsserver und ein Datenbankserver sind produktiv in einem gemeinsamen Brandabschnitt. Der andere Applikationsserver und der andere Datenbankserver im cold standby Modus und der Back-Up Server befinden sich in einem anderen gemeinsamen Brandabschnitt. Applikationsserver (redudant) und Datenbankserver (redundant) sind jeweils durch Paketfilter voneinander getrennt. Der Back-Up Server (Aufnahme und Bereitstellung der Datensicherungen) ist über einen Paketfilter von den Applikations- und Datenbankservern separiert.

3) Eine Kommunikation zu dem Datenbankserver (redundant) ist nur indirekt über den Applikationsserver (redundant) möglich. Eine direkte Kommunikation (außerhalb der ODBC-Verbindung) ist nicht möglich. Nur dieser Kommunikationsweg wird durch den Paketfilter erlaubt, alle anderen möglichen Verbindungen innerhalb der Serverstruktur sind verboten. Der Back-Up Server kann nur durch Applikationsserver und Datenbankserver angesprochen werden, die umgekehrte Kommunikationsrichtung ist nicht erlaubt. Nur dieser Kommunikationsweg wird durch den Paketfilter erlaubt, alle anderen möglichen Verbindungen innerhalb der Serverstruktur sind verboten.

4) Innerhalb der eigenen Serverräume (ITZ-Bund) befindliche Server für Infrastrukturdienste wie DNS, NTP, Windows Update (WSUS) sowie Virenscanner können über PAP-Strukturen vom MoFU-Netzwerk aus logisch erreicht werden. Administrative Updates/Patches werden auf einem aus dem MoFU-Netzwerk lesend erreichbaren Laufwerk zur Verfügung gestellt. Für die Systempflege/Administration kann aus dem MoFU-Netzwerk heraus lesend auf dieses Laufwerk zugegriffen werden, damit ist sichergestellt, dass keine Daten aus dem MoFU-Netzwerk herauskopiert werden können. Dieser lesende Zugriff wird durch einen Paketfilter geregelt. Grundsätzlich ist damit jede Kommunikation bis auf die benannte untersagt.

5) Das MoFU-Netzwerk verfügt über folgende Schnittstellen nach außen:

a. Die beiden SINA-WS im BiB sind über einen IP-Tunnel (netzseitig terminiert über SINA-Boxen) mit dem abgeschotteten MoFU-Netzwerk verbunden. Sie sind über eine PAP-Struktur (Kombination aus Paketfilter – Application Layer Gateway – Paketfilter) vom Servernetz getrennt. Dabei werden nur verschlüsselte Verbindungen über die SINA-Box zum Applikationsserver zugelassen. Alle anderen Zugriffe werden über die PAP-Struktur abgelehnt. Sie haben keine weitere Netzwerkanbindung. Sie befinden sich im zutrittsgesicherten MoFU-Arbeitsraum des BIB.

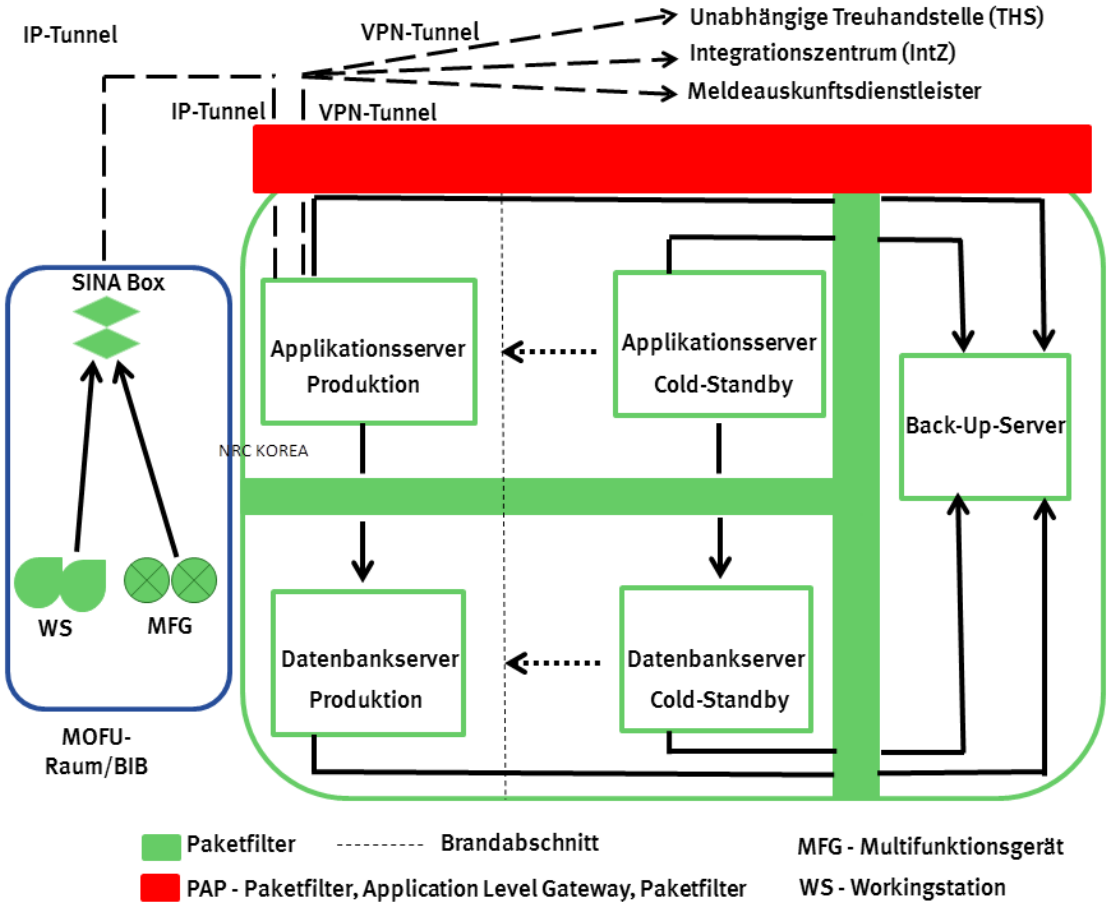
b. Die beiden Multifunktionsgeräte (Drucker / Scanner) sind ebenfalls ohne lokalen Speicher direkt über einen Tunnel (beidseitig terminiert über SINA-Boxen) mit dem MoFU-Netzwerk verbunden. Sie sind über eine PAP-Struktur (Kombination aus Paketfilter – Application Layer Gateway – Paketfilter) vom Servernetz getrennt. Dabei werden nur verschlüsselte Verbindungen über die SINA-Box mit dem (bidirektional) Applikationsserver zugelassen. Alle anderen Zugriffe werden über die PAP-Struktur abgelehnt. Sie haben keine weitere Anbindung über Netz bzw. USB. Sie befinden sich im zutrittsgesicherten MoFU-Arbeitsraum des BIB.

c. Der Datenaustausch mit den externen Schnittstellen THS, IntZ oder Meldeauskunft-Dienstleister erfolgt über VPN-Verbindungen mittels IPSec Client aus dem MoFU-Netzwerk heraus.

6) Nur auf den insgesamt fünf MoFU-Servern werden die IDAT und MDAT (MoFU-Daten) gespeichert, verarbeitet und genutzt. Wie unter 2) bereits benannt sind dies der Applikationsserver (redundant), der Datenbankserver (redundant) und der Backup-Server. Der Datenbankserver kann von den SINA-Workstations nur indirekt über den Applikationsserver angesprochen werden, ein direkter Zugriff ist nicht möglich. Die Multifunktionsgeräte werden von den SINA-Workstations über die SINA BOX und den Applikationsserver angesprochen; auf den Multifunktionsgeräten erzeugte Scans von Schriftgut werden direkt in das verschlüsselte Dokumentenverzeichnis des Applikationsserver gespeichert.

7) Diese Architektur stellt sicher, dass Verbindungen nur aus dem MoFU-Netzwerk „heraus“, nicht jedoch in das Netzwerk hinein aufgebaut werden können.

Die Schematische Darstellung 3 „IT-Netzwerk des Mortalitäts-Follow-Up“ zeigt die beschriebenen Zusammenhänge.



Schematische Darstellung 3: „IT-Netzwerk des Mortalitäts-Follow-Up“

6.2 VPN-Verbindungen

1) Der aktive MoFU-Applikationsserver baut für die Datenübermittlung mit der THS eine verschlüsselte VPN-Verbindung zum VPN-Router der THS im Netz der Universitätsmedizin Greifswald (UMG) auf („site-to-site“).

2) Der aktive MoFU-Applikationsserver baut für die Datenübermittlung zum Integrationszentrum (IntZ) eine verschlüsselte VPN-Verbindung zum zentralen VPN-Router des IntZ im Netz der Universitätsmedizin Greifswald (UMG) auf („site-to-site“).

3) Der aktive MoFU-Applikationsserver baut für die Datenübermittlung zum Meldeauskunft-Dienstleister eine verschlüsselte VPN-Verbindung in dessen Netz auf.

6.3 SINA-Workstations

1) Die elektronische Verarbeitung der IDAT und MDAT (MoFU-Daten) durch die MoFU-Mitarbeiter erfolgt nur über die MoFU-SINA-Workstations (MoFU-SINA-WS) auf den MoFU-Servern.

2) Die personenbezogene Anmeldung bzw. die Einwahl durch die MoFU-Mitarbeiter auf die SINA-WS erfolgt über eine personalisierte Smart-Card und mehrfach passwortgeschützt. Die Passwörter werden in regelmäßigen Abständen ausgetauscht.

3) Die MoFU-SINA-WS werden nur in den MoFU-Arbeitsräumen betrieben. Aufgrund einer Schließvorrichtung sind die WS nicht transportabel.

4) Die MoFU-SINA-WS sind so konfiguriert, dass sie nur die MoFU-Server erreichen und auf diese nur mittels RDP oder eines analogen Protokolls zugreifen können.

5) Alle Anschlüsse (z.B. USB) und Bauteile (z.B. DVD-RW) des MoFU-SINA-WS, die zum Anschluss oder Nutzung von mobilen Datenträgern genutzt werden können, sind abgeschaltet.

6) Die Administration der MoFU-Server erfolgt initial am Server direkt, später über eine Admin-Console im Rechenzentrum ITZ-Bund. Ein Wartungszugang von außerhalb des geschützten Rechenzentrums ist technisch ausgeschlossen.

6.4 Drucker und Scanner

1) Alle sonstige Verarbeitung von IDAT und MDAT (MoFU-Daten) erfolgt nur auf den in den MoFU-Arbeitsräumen genutzten Multifunktionsgeräten. Diese Geräte sind gesichert mit dem MoFU-Netzwerk verbunden. Diese Geräte sind nicht von Rechnern außerhalb des MoFU-Netzwerkes erreichbar. Diese Geräte legen keine lokalen Daten auf den SINA-WS ab. Alle Daten werden auf den gesicherten MoFU-Servern gespeichert.

2) Drucker, Scanner und Multifunktionsgeräte außerhalb der MoFU-Arbeitsräume kommen für die Verarbeitung von IDAT und MDAT (MoFU-Daten) nicht zum Einsatz.

6.5 Schriftgut mit IDAT und MDAT (MoFU-Daten)

1) Von außen empfangenes Schriftgut auf Papier (Todesbescheinigungen, Obduktionsbefunde, Briefe und ähnliches) mit personenbezogenen Daten zu den Teilnehmern der NAKO Studie wird sofort nach dem Eingang in abschließbaren sicheren Schränken im MoFU-Arbeitsraum im MoFU-Arbeitsraum aufbewahrt, bis die auf ihnen vorhandenen Daten entweder in vorgesehener Weise in die entsprechende Datenbank eingepflegt, oder nach unumkehrbarer Entfernung der personenidentifizierenden Daten pseudonymisiert, digitalisiert und sicher gespeichert wurden.

2) Die Daten und die pseudonymisiert, digitalisiert und sicher gespeicherten Kopien des Schriftgutes werden sodann unverzüglich an die THS oder das IntZ versandt.

3) Nach erfolgtem Versand der Daten oder der pseudonymisierten digitalisierten Kopien an die THS oder das IntZ und Erhalt der jeweiligen Empfangsbestätigung wird das zugrundeliegende Schriftgut unverzüglich, frühestens aber nach Ablauf von 24 Stunden

nach der Speicherung der auf dem Schriftgut vorhandenen Daten vernichtet (siehe auch Abschnitte 4.2.3 (13) und 6.6 (2).

4) Von außen empfangenes Schriftgut wird vernichtet nach Schreddern im MoFU-Arbeitsraum durch Entsorgung in einer Datentonne, deren Inhalt durch einen externen Dienstleister nach DIN 66399 mit mind. Schutzklasse 3 Sicherheitsniveau 4 vernichtet wird. Die Vernichtung per Schredder mit anschließender Entsorgung ist von einem MoFU-Mitarbeiter mit Zeitangaben in einem fortlaufend zu führenden Protokoll zu vermerken.

6.6 Betriebssystem des MoFU-Servers

1) Auf den MoFU-Servern ist Windows als Server-Betriebssystem installiert.

2) IDAT und MDAT (MoFU-Daten) werden grundsätzlich PGP-verschlüsselt abgelegt und gesichert. Der erforderliche private Schlüssel steht ausschließlich den Mitarbeitern des MoFU zur Verfügung.

3) Die Datenbanktabellen werden mit „Always Encrypted“-Mechanismen unter MS-SQL 2016 gesichert. Die Verschlüsselung basiert auf einem vollständigen Zertifikat für die Nutzer des MoFU sowie einem für Notfälle hinterlegten vollständigen Zertifikat für die Datenbankadministration. Hierdurch sind die Daten auch nach Systemfehlern / Bedienungsfehlern die das installierte Zertifikat beschädigen können geschützt und zugreifbar. Der Ordner in dem die Datenbankanwendung und ggf. anfallende temporäre Daten abgelegt sind, ist mit encrypted file system (efs) unter Windows verschlüsselt. Die vollständigen Zertifikate sind den Nutzern des MoFU zugeordnet; ein vollständiges Zertifikat zur Wiederherstellung ist für Notfälle hinterlegt.

4) Zusätzlich werden die Dateiablagen der virtuellen Server mit Bitlocker-Verschlüsselung grundgesichert. Das Passwort liegt beim Windows-Administrator; der Wiederherstellungsschlüssel ist für Notfälle hinterlegt.

5) Hinterlegt in (3) und (4) bedeutet, dass im Notfall – unter Beteiligung der Mitarbeiter des MoFU - gemeinsam auf diese Schlüssel zugegriffen werden darf. Der Stick mit dem Schlüssel ist in einem verschlossenen Umschlag in einem gesicherten Stahlschrank in einem der Rechenzentren des ITZBund am Standort Wiesbaden verwahrt. Zugang ist nur gemeinsam möglich (Organisatorische Regelung im RZ-Betrieb).

6.7 Anwendersoftware

1) Als Internet-Browser zur Nutzung der Webportale der THS und des IntZ wird ein Microsoft-Produkt genutzt, da dieser über Microsoft-Update aktualisiert werden kann.

2) Der MoFU-Datenbankserver läuft unter MS-SQL und verschlüsselt die Datenbanktabellen auf Applikationsebene.

3) Der MoFU-Applikationsserver verfügt über MS-Access für den Zugriff auf die verschlüsselten Datenbanktabellen des MS-SQL-Servers sowie einen Terminalserver für den Zugriff der MoFU-SINA WS.

6.8 Datenaustauschformat

1) Der Datenaustausch mit THS, IntZ und Meldeauskunft-Dienstleister erfolgt über Upload- und Download Verfahren.

2) Mit THS und IntZ erfolgt der Datenaustausch mit XML-Dateien (siehe auch Abschnitt 7.1). Mit dem Meldeauskunft-Dienstleister erfolgt der Datenaustausch mit VSC-Dateien.

7 Technische Maßnahmen: Prozesse der Datenverarbeitung

7.1 Datenübertragung

1) Die Datenübertragung zwischen dem Mortalitäts-Follow-Up und der THS oder dem IntZ erfolgt mittels nach aktuellem PGP Standard verschlüsselter Dateien. Der Austausch der öffentlichen Schlüssel erfolgt persönlich oder über die VPN-Verbindung. Mit THS und IntZ wird ein regelmäßiger Tausch der Schlüssel vereinbart. Dabei darf die Gültigkeitsdauer der Schlüssel nicht mehr als 2 Jahre übersteigen.

2) Das Mortalitäts-Follow-Up überträgt die Daten von und zur THS oder von und zu dem IntZ durch Download bzw. Upload der verschlüsselten Dateien zu den Webportalen von THS und IntZ.

3) Die Datenübertragung erfolgt durchgehend verschlüsselt nach aktuellem PGP Standard über VPN.

4) Die Datenübertragung zwischen dem Mortalitäts-Follow-Up und dem Meldeauskunft-Dienstleister erfolgt ebenfalls über VPN mit Verschlüsselung nach aktuellem PGP Standard.

7.2 Datensicherung

1) Die regelmäßige Datensicherung erfolgt durch den Back-Up-Server, nicht auf Bändern. Über die Datensicherung wird regelmäßig Protokoll geführt.

2) Die IDAT und MDAT (MoFU-Daten) werden auf dem Back-Up-Server nur verschlüsselt gespeichert.

3) Die Aufbewahrungsfrist für Datensicherungen soll 1 Jahr und darf 2 Jahre nicht überschreiten. Die Daten werden roulierend gesichert. Sicherungen je Arbeitstag werden im Folgemonat überschrieben. Die monatliche Sicherung wird jeweils aktuell überschrieben. Damit wird auch für die Back-Ups die im Rahmen der NAKO Gesundheitsstudie festgelegte Löschfrist von 4 Wochen grundsätzlich eingehalten. Dabei ist anzumerken, dass das produktive System der MoFU in einem Brandabschnitt des Rechenzentrums untergebracht ist, während der Back-Up-Server und die cold-standby-Infrastruktur in einem anderen, getrennten Brandabschnitt in einem zweiten Rechenzentrum installiert sind. Die Daten (produktiv und Backup) liegen somit in zwei verschiedenen Rechenzentren und damit auch in zwei Brandabschnitten, in den Räumlichkeiten des Statistischen Bundesamtes am Standort Wiesbaden.

4) Eine weitergehende elektronische Aufbewahrung der IDAT und MDAT (MoFU-Daten) außerhalb der Anwendung findet nicht statt.

8 Technische Maßnahmen: Dokumentation

1) Ein für die Mitarbeiter des ITZBund bestimmtes Betriebshandbuch, in dem die gesamte zur Datenverarbeitung im Mortalitäts-Follow-Up der NAKO Gesundheitsstudie eingesetzte IT-Hardware und Software dokumentiert ist, wurde erstellt und verbleibt beim ITZBund.

2) Ein für die MoFU-Mitarbeiter bestimmtes Handbuch zur Bedienung aller Geräte im MoFU-Arbeitsraum und aller über diese zugängliche Software einschließlich der Datenbanken durch die MoFU-Mitarbeiter wurde erstellt und verbleibt im MoFU-Arbeitsraum.

9 Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BAnzAT	Bundesanzeiger Amtlicher Teil
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSV	Comma Separated Values
DBMS	Database Management System
DNS	Domain Name System
ICD	International Classification of Diseases and Related Health Problems
ID-ADL	Pseudonym für Datenübergabe an Meldeauskunft-Dienstleister
IDAT	Satz personenidentifizierender Daten
ID-TU	Pseudonym bei Todesursachenerhebung
ID-V	Pseudonym bei Vitalstatuserhebung
IntZ	Integrationszentrum
ITZBund	Informationstechnikzentrum Bund = der IT-Dienstleister der Bundesbehörden
MODYS	Software zur Verwaltung von Teilnehmern in den Studienzentren der NAKO
MoFU	Mortalitäts-Follow-Up
MS-SQL	Microsoft SQL Structured Query Language
NTP	Network Time Protocol
PAP	Paketfilter, Application Level Gateway
PGP	Pretty Good Privacy
PStG	Personenstandsgesetz
RDP	Remote Desktop Protocol
sftp	Secure File Transfer Protocol
SINA-WS	Die SINA Workstation ist ein Fat Client mit Kryptodateisystem
SZ	Studienzentrum
THS	Unabhängige Treuhandstelle
TLS	Transport Layer Security
UMG	Universitätsmedizin Greifswald
VPN	Virtual Privacy Network
VSC	Versus Programing Language
WHO	World Health Organization
WSUS	Microsoft Windows Update Services
XML	Extensible Markup Language

10 Anhang

11 Separate Anlagen

11.1 Synopse: Rechtliche Regelungen des Zugangs wissenschaftlicher Forschung zur Todesbescheinigung nach Bundesländern

11.2 Beispiel: Bayerische Todesbescheinigung

11.3 Bevollmächtigung des Bundesinstituts für Bevölkerungsforschung zum Abschluss von Unterauftragsverhältnissen für Meldeauskünfte durch den Vorstand der NaKo e.V. vom 09.05.2017 (nicht veröffentlicht)

11.4 Muster-Anschreiben an die Gesundheitsämter zur Anforderung der Todesbescheinigungen