Rahmendatenschutzkonzept DKFZ

Personenbezogene Daten für die Krebsforschung

Version 2.0, Februar 2017

Hauptautoren:

- Heidrun Binder
- Holger Haas
- Dr. Harald Aamot (Version 1)
- Prof. Benedikt Brors

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Präambel

Mit diesem Rahmendatenschutzkonzept (RDSK) stellt sich das Deutsche Krebsforschungszentrum (DKFZ) seiner Verantwortung, langfristig und nachhaltig Forschung mit personenbezogenen Daten im onkologischen Umfeld zu ermöglichen und gleichzeitig die Vertraulichkeit dieser Daten zu gewährleisten und die Rechte und Interessen der Betroffenen zu schützen.

Viele Krebspatienten[1], häufig in existentiellen Notsituationen, erlauben die Benutzung ihrer persönlichen Daten, um die Forschung zu unterstützen und zukünftigen Patienten zu helfen. Das DKFZ und seine Forscher wollen diesem Vertrauensvorschuss von Patienten und Probanden gerecht werden.

Personenbezogene Daten wie Genomdaten und klinische Daten haben zum Teil erhebliche Aussagekraft über die betreffende Person. Sie berühren private und intime Lebenssphären in ihrem Kerngehalt und somit auch die Stellung und Würde des Einzelnen gegenüber Gesellschaft und Staat. Insbesondere Genomdaten haben eine große und weit in die Zukunft reichende Aussagekraft, die sich nicht nur auf die Person des Spenders und dessen Krankheitsdispositionen, Persönlichkeitseigenschaften und Verhaltensweisen erstreckt, sondern auch auf nahe Verwandte und Kinder des Spenders. Für die Betroffenen und ihre Verwandten besteht u.a. die Gefahr der Re-Identifizierung, der Verletzung ihrer Privatsphäre sowie der legalen oder illegalen Verwendung der Daten durch Dritte zu ihrem Nachteil. Diese Gefahren können u.a. von Versicherungsunternehmen, Arbeitgebern oder Regierungen bzw. staatlichen Einrichtungen ausgehen.

Besondere Verantwortung erwächst den Forschern aus einer doppelten Ungewissheit: Zum einen ist das Aussagepotenzial von Genomdaten bisher nur teilweise bekannt. Zum anderen sind die zukünftigen technischen Möglichkeiten der redlichen wie unredlichen Gewinnung, Speicherung, Verarbeitung und Nutzung von Genom- und anderen Personendaten sowie die möglichen Folgen für Individuen und Gesellschaft nicht vorhersehbar.

Forschung mit Personendaten, insbesondere mit so sensiblen Daten wie Genomdaten, ist ein langfristiges gesamtgesellschaftliches Projekt. Eine unersetzliche Ressource dafür ist das Vertrauen, das aktuelle und zukünftige Patienten und Probanden sowie die Öffentlichkeit dem DKFZ und seinen Forschern entgegenbringen.

Mit dieser Ressource verantwortungsvoll und sorgfältig umzugehen und sie weder kurz- noch langfristig zu gefährden, ist Pflicht aller Beteiligten. Zur Verantwortung eines jeden einzelnen Beteiligten gehört vorausschauende Sorgfalt und die komplexe Einschätzung und Berücksichtigung der Risiken eigenen Handelns gemäß dem Sinn und Geiste dieses Rahmendatenschutzkonzepts und seiner Präambel.

[1] Sofern in diesem Rahmendatenschutzkonzept lediglich die männliche Personenbezeichnung verwendet wird, erfolgt dies aufgrund der besseren Lesbarkeit und bezieht sich gleichermaßen auf weibliche und männliche Personen.

1. Einleitung

1.1. Motivation und Problematik

Die Durchführung von wissenschaftlichen Forschungsvorhaben mit Patienten- und Probandendaten ist von essentieller Bedeutung für die Weiterentwicklung der Diagnose-, Behandlungs- und Präventionsmöglichkeiten in einem modernen Gesundheitswesen. Der Informationsfluss zwischen Labor (Grundlagenforschung) und Anwendung am Patienten (Patientenversorgung) wird als Translation bezeichnet und ist der Motor der klinischen Forschung. Translationale Forschung ist u.a. auch auf Forschung mit Daten von Menschen ausgerichtet, an die erhöhte Datenschutz-anforderungen gestellt werden.
Das vorliegende Konzept ist im DKFZ unter der Beteiligung der Bereiche Datenschutz, IT-Sicherheit, Qualitätsmanagement klinischer und kliniknaher Forschung, IT Core Facility, Genomforschung, Radiologie, Epidemiologie und mit Unterstützung der EURAT (Ethische und Rechtliche Aspekte der Totalsequenzierung des menschlichen Genoms)-Projektgruppe des Marsilius-Kollegs der Universität Heidelberg entstanden.

1.2. Zielsetzung

Das Rahmendatenschutzkonzept soll den Datenschutz und die IT-Sicherheit personenbezogener Daten in der Krebsforschung gewährleisten. Es definiert und regelt die technischen und organisatorischen Datenschutz- und IT-Sicherheitsmaßnahmen um die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen. Die IT-Sicherheit betrachtet die mehr technischen Aspekte der Datenverarbeitung, der Datenschutz das rechtliche Umfeld.
Mit dem Rahmendatenschutzkonzept verfolgt das DKFZ das Ziel, Forschung mit genetischen und anderen personenbezogenen Daten in nationalen und internationalen Zusammenhängen zu ermöglichen, und dabei gleichzeitig

- die Rechte und Interessen der Betroffenen und ihrer Verwandten zu schützen,
- die Vertraulichkeit persönlicher Daten und informationelle Selbstbestimmung zu gewährleisten,
- das Vertrauen der Patienten bzw. Probanden und der Öffentlichkeit gegenüber dem DKFZ als Institution und jedem seiner Forscher zu rechtfertigen und zu bewahren,
- redliche und verantwortungsvolle Forschungskultur auf allen Ebenen zu stärken,
- das DKFZ und seine Forscher vor rechtlichen Sanktionen zu bewahren indem Fehlverhalten vermieden wird,
- die Werte und Prinzipien der liberalen, demokratisch-rechtstaatlichen Gesellschaftsordnung zu achten.

1.3. Geltungsbereich

Das vorliegende Rahmendatenschutzkonzept gilt für alle Beschäftigten des DKFZ, die mit personenbezogenen Daten arbeiten. Die Verantwortlichkeiten sind in Kapitel 3 definiert. Der IT-Verbund umfasst alle Forschungsschwerpunkte und zentrale Einheiten des DKFZ einschließlich der entsprechenden Bereiche an den DKTK-Standorten, die von DKFZ-Mitarbeitern verantwortet werden.

Die Vorgaben und Richtlinien für die Verarbeitung von personenbezogenen Daten sind zu befolgen. Die entsprechenden Maßnahmen sind mit dem Datenschutzbeauftragten des DKFZ abzustimmen und sind entweder in projektspezifischen Datenschutzkonzepten zu beschreiben und umzusetzen, oder die in dem vorliegenden Rahmendatenschutzkonzept definierten Maßnahmen sind umzusetzen.

1.4. Allgemeine Definitionen

1.4.1. Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) (§ 3 Abs. 1 BDSG und § 3 Abs. 1 LDSG-BW). Beispiele personenbezogener Daten sind Name, Geschlecht, Geburtsdatum, Initialen, Einkommen, Krankheitsgeschichte, Wohnort, Größe der Person. Je umfassender eine Datenansammlung ist, desto größer ist die theoretische Möglichkeit, diese einer bestimmten Person zuzuordnen.

1.4.2. Personenidentifizierende Daten

Personenidentifizierende Daten (IDAT) sind Angaben, die den Rückschluss auf eine eindeutig bestimmbare natürliche Person im Normalfall unaufwändig erlauben. Dieser Datentyp wurde von der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF) e.V. eingeführt und ist eine Untermenge der personenbezogenen Daten. Als Orientierung kann die Aufzählung des TMF Leitfadens dienen (s. Glossar).

1.4.3. Medizinische Daten

Medizinische Daten des Patienten umfassen sämtliche bei der Behandlung anfallenden medizinischen Informationen wie Diagnosen, Anamnesen, Laborwerte, Therapien, verordnete Medikamente, Operationen etc. sowie evtl. für die Forschung zusätzlich erhobene Daten.

1.4.4. Anonymisieren

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 6 BDSG und § 3 Abs. 6 LDSG-BW).
Für die Beurteilung, ob der erforderliche Aufwand zur Identifizierung unverhältnismäßig ist, kommt es auf die Verhältnisse im Einzelfall an. Dabei sind insbesondere der wirtschaftliche oder sonstige Vorteil der infrage stehenden Daten für potenzielle Interessenten, deren Bereitschaft zur Leistung eines unverhältnismäßigen Aufwands und die den potenziellen Interessenten zur Verfügung stehenden Ressourcen wie weiteres Wissen über die Daten sowie technische Möglichkeiten der Re-Identifizierung, zu berücksichtigen.
Die Qualität der Anonymisierungsprozedur hängt von verschiedenen Einflussfaktoren ab. Entscheidend hierfür sind der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Mächtigkeit der Menge, in der sich die Person verbirgt und die Verkettungsmöglichkeit von einzelnen Transaktionen

derselben Person. Auch konkrete Einzelangaben in einem Datensatz oder einer Transaktion sind für die Qualität der Anonymisierungsprozedur von Bedeutung und können die Mächtigkeit der Menge, in der sich die Person verbirgt, verringern. Sind im Wertebereich Angaben vorhanden, die die Anonymität gefährden, müssen sie mit anderen zusammengefasst werden. Ist eine solche Veränderung aus technischen oder inhaltlichen Gründen nicht möglich, kann keine Anonymität erreicht werden.
(Quelle: https://www.datenschutz-praxis.de/fachartikel/anonymisierung-und-pseudonymisierung-von-kundendaten/, abgerufen am 07.10.2016)

1.4.5. Pseudonymisieren

Pseudonymisieren ist das Ersetzen der personenidentifizierenden Daten durch ein Kennzeichen, ein Pseudonym (PSN) zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§ 3 Abs. 6a BDSG und § 3 Abs. 7 LDSG-BW).
Allgemein bezeichnet Pseudonymisierung eine Prozedur, die personenbezogene Daten durch eine Zuordnungsvorschrift derart verändert, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.
Dazu werden beispielsweise die Identifikationsdaten (IDAT) durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym PSN) überführt. Unterschiedliche Stufen einer Pseudonymisierung werden bei den zentralen Maßnahmen beschrieben.
Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wieder herstellen zu können.
Mit Pseudonymen versehene Daten sind jedoch weiterhin personenbezogene Daten, da sie einer bestimmten oder bestimmbaren Person zugeordnet werden können. Allerdings sind die Daten für denjenigen, der die Zuordnungsvorschrift nicht kennt, der also insbesondere nicht über die Referenzliste verfügt, so gut wie anonym.
Das Mittel der Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo die wissenschaftliche Aufgabe mit anonymisierten Daten nicht erfüllt werden kann.
(Quelle: https://www.datenschutz-praxis.de/fachartikel/anonymisierung-und-pseudonymisierung-von-kundendaten/, abgerufen am 07.10.2016)

1.4.6. Data Transfer Agreement

In einem Data Transfer Agreement wird definiert, welche Informationen (=Daten) im Sinne der Vereinbarung vertraulich zu behandeln sind. In dieser Vereinbarung wird geregelt:

- wer Informationsgeber bzw. Informationsnehmer ist,
- zu welchem Zweck die Daten ausgetauscht werden,
- wie die Daten ausgetauscht werden und wie sie verarbeitet bzw. weitergegeben werden dürfen sowie
- der zeitliche Rahmen, für den diese Vereinbarung gilt.

1.4.7. EURAT Kodex

In den letzten Jahren ist – bedingt durch komplexer gewordene Forschungsmethoden und -ergebnisse – verstärkt daran erinnert worden, dass die Praxis wissenschaftlichen Arbeitens durch ethische Grundsätze geleitet werden soll.

Um dieser Forderung nachzukommen, haben Heidelberger Wissenschaftler das interdisziplinäre Gemeinschaftsprojekt „EURAT – Ethische und rechtliche Aspekte der Totalsequenzierung des menschlichen Genoms“ aufgelegt. Im Juni 2013 hat die EURAT-Projektgruppe ihre Stellungnahme zu ethischen und rechtlichen Konsequenzen der Totalsequenzierung des menschlichen Genoms abgegeben. Sie wurden als „Eckpunkte für eine Heidelberger Praxis der Ganzgenomsequenzierung“ veröffentlicht, eine Aktualisierung dieser Stellungnahme erfolgte im November 2015.

Die EURAT-Projektgruppe betont, dass der Forscher nicht nur die Pflicht hat, die Wissenschaft und Gesellschaft über seine Forschung, ihre Methoden, Ziele und Ergebnisse zu unterrichten, sondern auch eine Verpflichtung den untersuchten Personen und ihren Familien gegenüber, die Daten schonend zu ihrem Wohl zu nutzen und gegen das Mitwissen Unberechtigter abzuschirmen. Deshalb wurde ein Kodex für Wissenschaftler, die an der Totalsequenzierung, insbesondere von Patienten-Genomen, beteiligt sind, verabschiedet. Dieser Kodex kann für die Wissenschaftler als eine Art Äquivalent zum hippokratischen Eid der Ärzte gesehen werden. Er enthält – neben den allgemeinen ethischen Grundsätzen, nach denen zu handeln ist (zum Beispiel die Achtung der Person, Selbstbestimmung des Patienten, Schadensvermeidung, Gute Wissenschaftliche Praxis und Schutz künftiger Generationen) – detaillierte und verbindliche Handlungsrichtlinien.

1.5. Rechtsgrundlage, rechtliche Rahmenbedingungen

Die Forschung mit personenbezogenen Daten bewegt sich im Spannungsfeld zwischen dem Interesse der Forscher, dem Bedarf der Allgemeinheit an einer möglichst umfassenden Forschung und dem Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). Dabei sind nach dem Grundsatz der Datensparsamkeit so wenig personenbezogene Daten wie möglich zu erheben, zu speichern bzw. zu verarbeiten, um Einschränkungen des Rechts auf informationelle Selbstbestimmung von vornherein zu minimieren. Daraus folgt, dass personenbezogene Daten zu anonymisieren sind, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Identifikationsmerkmale gesondert zu speichern. Sie dürfen mit den anderen Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert. Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung bearbeitet werden.

Trotz der durch das Grundgesetz gewährleisteten Forschungsfreiheit (Artikel 5 Grundgesetz) gilt auch für die wissenschaftliche Forschung mit personenbezogenen Daten wegen des ebenfalls maßgeblichen Rechts auf informationelle Selbstbestimmung des Betroffenen das grundsätzliche Verbot mit Erlaubnisvorbehalt. Rechtlich unproblematisch ist die Forschung mit anonymisierten Daten oder nach hinreichend konkreter und freiwillig erteilter Einwilligung des Betroffenen (ausgeübtes Recht auf informationelle Selbstbestimmung). Diese beiden Möglichkeiten allein würden allerdings eine Vielzahl an Forschungsvorhaben, für die ein großes öffentliches Interesse besteht, verhindern. Daher hat der Gesetzgeber in Bund und Ländern besondere

Erlaubnistatbestände für die Forschung geschaffen. Diese Forschungsregelungen legen die rechtlichen Vorgaben fest, unter denen Einschränkungen des Rechts auf informationelle Selbstbestimmung zum Zwecke der wissenschaftlichen Forschung möglich sind. Kern sind dabei Bedingungen, die eine Forschung ohne Einwilligung des Betroffenen erlauben. In Baden-Württemberg beurteilt sich die Zulässigkeit der Forschung mit Patientendaten nach dem im DKFZ als Stiftung öffentlichen Rechts des Landes Baden-Württemberg geltenden Landes-Datenschutzgesetz (LDSG-BW), bzw. in Anlehnung an das Bundesdatenschutzgesetz (BDSG).

Für dieses Rahmendatenschutzkonzept gelten die §§ 2-6, 9, 11-16, 18-20, 21-25, 33, 34 und 35 LDSG-BW. Als für die DKFZ-Forschung besonders relevant sind die im Folgenden genannten Rechtsnormen:

- § 4 Zulässigkeit der Datenverarbeitung
- § 19 Übermittlung für Zwecke der wissenschaftlichen Forschung
- § 33 Verarbeitung besonderer Arten personenbezogener Daten
- § 34 Zweckbindung bei der Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen
- § 35 Verarbeitung personenbezogener Daten durch Forschungseinrichtungen.

Links zu allen genannten Rechtsvorschriften sind im Anhang zu finden. Insbesondere ist Folgendes zu beachten:

Gemäß **§ 4 LDSG-BW** ist nach erteilter Einwilligung des Patienten die Nutzung seiner personenbezogenen Daten für ein Forschungsprojekt zulässig. Bei Abgabe der Einwilligungserklärung müssen die Patienten sachgerecht über die Zielsetzung des Forschungsprojektes, die beteiligten Stellen und Personen sowie über die Art der Datenverarbeitung informiert werden. Die Aufklärungspflicht umfasst bei einer beabsichtigten Übermittlung auch den Empfänger der Daten. Die Erklärung muss schriftlich oder elektronisch erfolgen, freiwillig und mit Wirkung für die Zukunft widerrufbar sein. In diesem Zusammenhang ist zu erwähnen, dass eine ärztliche Behandlung nicht von der Erteilung einer Einwilligung in die Verwendung der Daten für Forschungszwecke abhängig gemacht werden darf. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.
Für eine Stelle wie das DKFZ besteht, unter Auflagen, gemäß **§35 Abs. 1 – 3 LDSG-BW,** die Möglichkeit, personenbezogene Daten auch ohne Einwilligung des Betroffenen zu verarbeiten, wenn „der Zweck des Forschungsvorhabens auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann." Diese Regelung stellt keine Offenbarungsbefugnis gemäß § 203 StGB dar, die strafrechtlich und berufsrechtlich geregelte ärztliche Schweigepflicht wird hierdurch nicht aufgehoben. Von der ärztlichen Schweigepflicht sind alle Daten geschützt, die im direkten Behandlungskontext erhoben werden.
Darüber hinaus hat sich das DKFZ dem EURAT-Kodex verpflichtet, so dass die oben genannte Möglichkeit nur als äußerstes Mittel und nicht für Ganzgenomdaten in Betracht gezogen wird. Vielmehr ist es Ziel – wo immer möglich – Daten nur auf der Grundlage einer Einverständniserklärung zu verarbeiten.

Die Translation von Forschungsergebnissen in die klinische Anwendung stellt ebenfalls hohe Ansprüche in Bezug auf die Erfüllung rechtlicher Anforderungen an eine wissenschaftliche Einrichtung. Durch die enge Vernetzung mit klinischen Partnern sind in bestimmten Fällen neben dem LDSG auch die Vorschriften des Medizinproduktegesetzes (MPG) und des Arzneimittelgesetzes (AMG) zu berücksichtigen, abhängig davon, ob die zu betrachtenden Daten z.B. bei der Entwicklung eines Medizinproduktes oder im Rahmen einer klinischen Prüfung von Arzneimitteln entstehen. Beide Gesetze sehen zwingend die schriftliche Einverständniserklärung als Voraussetzung der Zulässigkeit der Verarbeitung der Daten vor.
In Verbundprojekten über mehrere Bundesländer bzw. Ländergrenzen hinweg wird das Bundesdatenschutzgesetz als Rechtsnorm herangezogen.

1.6. Rechte der Betroffenen

Personen, deren Daten in der Forschung verwendet werden, haben gemäß § 5 LDSG-BW insbesondere die folgenden Rechte:

- Recht auf Auskunft über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und den Zweck der Verarbeitung.
- Recht auf Berichtigung, wenn unrichtige Daten gespeichert werden.
- Recht auf Sperrung, soweit die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
- Recht auf Löschung, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden. An die Stelle einer Löschung tritt eine Sperrung, soweit Aufbewahrungsfristen entgegenstehen, der Grund zur Annahme besteht, dass die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigen würde oder die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohen Aufwand möglich ist.
- Recht auf Einwendung gegen die Datenverarbeitung wegen der besonderen persönlichen Situation des Betroffenen, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift verlangt wird.
- Recht auf Schadensersatz wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten.

Diese Rechte können nicht durch Verträge oder sonstige Rechtsgeschäfte ausgeschlossen oder beschränkt werden.
Darüber hinaus kann sich der Betroffene zu Fragen des Datenschutzes auch an den betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB), den Landesbeauftragten für Datenschutz oder die jeweils zuständige Aufsichtsbehörde wenden. Niemand darf benachteiligt oder gemaßregelt werden, weil er sich an einen Datenschutzbeauftragten oder die Aufsichtsbehörde gewandt hat. Form- und Fristerfordernisse bestehen nicht.

2. Schutzbedarfsklassen und Schutzbedarfsfeststellung

2.1. IT-Sicherheit und Datenschutz

Zum Schutz personenbezogener Daten sind von den Daten verarbeitenden Stellen technische und organisatorische Maßnahmen zu treffen, um die Ausführung der gesetzlichen Vorschriften zu gewährleisten. Insbesondere sind die sogenannten Datenschutzkontrollen zu beachten. Als Orientierungshilfe für die Umsetzung von Maßnahmen für die Datenschutzkontrollen haben im deutschsprachigen Raum die Standards zur Informationssicherheit und zum Notfallmanagement sowie die IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) in der öffentlichen Verwaltung und vielen Unternehmen weithin Anerkennung und Anwendung gefunden. Hier werden auch die folgenden Grundwerte definiert:

1. **Vertraulichkeit** von Daten und Informationen: Unbefugte haben darauf keinen Zugriff, weder auf gespeicherte Daten noch auf übertragene Daten.
2. **Integrität** von Daten: Unbefugte oder unbemerkte Veränderungen von Daten, sei es durch Personen oder technische Fehler, sind ausgeschlossen.
3. **Verfügbarkeit** von Daten und Systemen: Daten und Systeme stehen verlässlich zur Verfügung, wenn sie gebraucht werden, Systemausfälle werden verhindert, der Zugriff auf Daten wird innerhalb eines vereinbarten Zeitrahmens gewährleistet.

Der Aufwand für die Sicherheitsmaßnahmen muss in einem angemessenen Verhältnis zum erforderlichen Sicherheitsniveau stehen.

Im DKFZ sind insbesondere die Grundwerte Vertraulichkeit und Integrität relevant. Die Verfügbarkeit hat für den Forschungsbetrieb eine weniger große Bedeutung. Es ist auch zu beachten, dass ein Zusammenhang zwischen Verfügbarkeit und den anderen Grundwerten, z.B. im Falle einer Katastrophe (Feuer, Wasser) besteht.

2.2. Schutzbedarfsfeststellung und Schutzbedarfsklassen

Die Schutzbedarfsfeststellung hängt davon ab, welcher Schaden entstehen kann, wenn die Grundwerte der Informationssicherheit verletzt werden.
Die IT-Grundschutz-Vorgehensweise des BSI definiert drei Schutzbedarfsklassen:

2.2.1. Schutzbedarfsklasse "normal"

Schutzbedarfsklasse „normal“ (SBK-N) bedeutet, dass der Schutz personenbezogener Daten insofern gewährleistet sein muss, so dass keine Gefahr besteht, den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen zu beeinträchtigen.

2.2.2. Schutzbedarfsklasse "hoch"

Schutzbedarfsklasse „hoch“ (SBK-H) bedeutet, dass der Schutz personenbezogener Daten hohen Anforderungen genügen muss. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

2.2.3. Schutzbedarfsklasse "sehr hoch"

Schutzbedarfsklasse „sehr hoch“ (SBK-SH) bedeutet, dass der Schutz personenbezogener Daten gewährleistet sein muss, so dass es zu keiner Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen kann. Auch eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, für die datenverarbeitende Stelle denkbar gilt es zu vermeiden.

Der Schutzbedarf kann für die einzelnen Grundwerte der IT-Sicherheit unterschiedlich sein.
Eine messbare klare Abgrenzung der Schutzbedarfsklassen ist vor allem in den Bereichen Integrität und Vertraulichkeit schwierig. Anhaltspunkt für die Einstufung sollten die Schadensauswirkungen für das DKFZ, seine Beschäftigten, seine Kooperationspartner und die Patienten bzw. Probanden (d.h. die Betroffenen) sein.

2.3. Generelle Vorgehensweise bei der Schutzbedarfsfeststellung

Angelehnt an die gängige Praxis des Risikomanagements im DKFZ müssen für jedes Projekt die zu verarbeitenden Daten bzgl. ihres Informationsgehalts untersucht und potenzielle Risiken und Gefährdungen identifiziert werden. Es wird beurteilt, wie wahrscheinlich der Eintritt eines Schadensereignisses ist und welches Ausmaß der Schaden im Falle des Eintritts annehmen könnte.
Die Risikoanalyse bildet die Grundlage für die Einstufung der Daten in eine Schutzbedarfsklasse, woraus die zu ergreifenden Maßnahmen resultieren. Diese Maßnahmen zielen sowohl auf die bewusste Verringerung der Eintritts-wahrscheinlichkeit als auch auf die Begrenzung der Auswirkungen bei Eintritt von Risiken ab.
Generell ist für jedes Projekt mit personenbezogenen Daten eine Verfahrensmeldung bei dem Datenschutzbeauftragten des DKFZ einzureichen.

2.3.1. Bestandsprojekte

Mit Bestandsprojekten sind in diesem Zusammenhang Projekte gemeint, die zum Zeitpunkt des Inkrafttretens des Rahmendatenschutzkonzeptes bereits durchgeführt werden.

Im Einzelnen sind bei Bestandsprojekten folgende Schritte durchzuführen:

1. Die einzelnen Datenpools (Sammlung von Daten, die gleichen Kriterien entsprechen, z.B. nur Daten ohne personenidentifizierende Merkmale) und Verarbeitungsschritte sind einer Risikoanalyse inkl. Prüfung eines eventuell vorhandenen Data Transfer Agreements (DTA) zu unterziehen.
2. Die Risikoanalyse führt zu einer Einordnung in eine Schutzbedarfsklasse. Diese kann für die unterschiedlichen Datenpools verschieden sein. Sollte die wissenschaftliche Aufgabe nach Umsetzung der erforderlichen Maßnahmen der ermittelten Schutzbedarfsklasse nicht durchführbar sein, sind die Daten in kritische und weniger kritische Datenpools aufzuteilen und erneut zu analysieren entsprechend einem neuen Projekt (s.u.). Dabei werden Datenpools, die personenidentifizierende Daten (IDAT) enthalten, immer in SBK-SH eingestuft.

3. Aus der ermittelten Schutzbedarfsklasse ergeben sich die Schutzmaßnahmen, die umzusetzen sind.
4. Unter Berücksichtigung der finalen Schutzbedarfsklassen ist in einer abschließenden Risikoanalyse das Restrisiko zu bewerten.
5. Für das Projekt ist eine Verfahrensmeldung bei dem Datenschutzbeauftragten des DKFZ einzureichen.
6. Wenn die Daten aus rechtlichen oder projektspezifischen Gründen über das Projektende hinaus aufbewahrt werden müssen, ist für diesen Aufbewahrungszeitraum eine erneute Risikoanalyse durchzuführen.

Die Verfahrensweise bei Bestandsprojekten ist in Abbildung 1 grafisch aufbereitet.

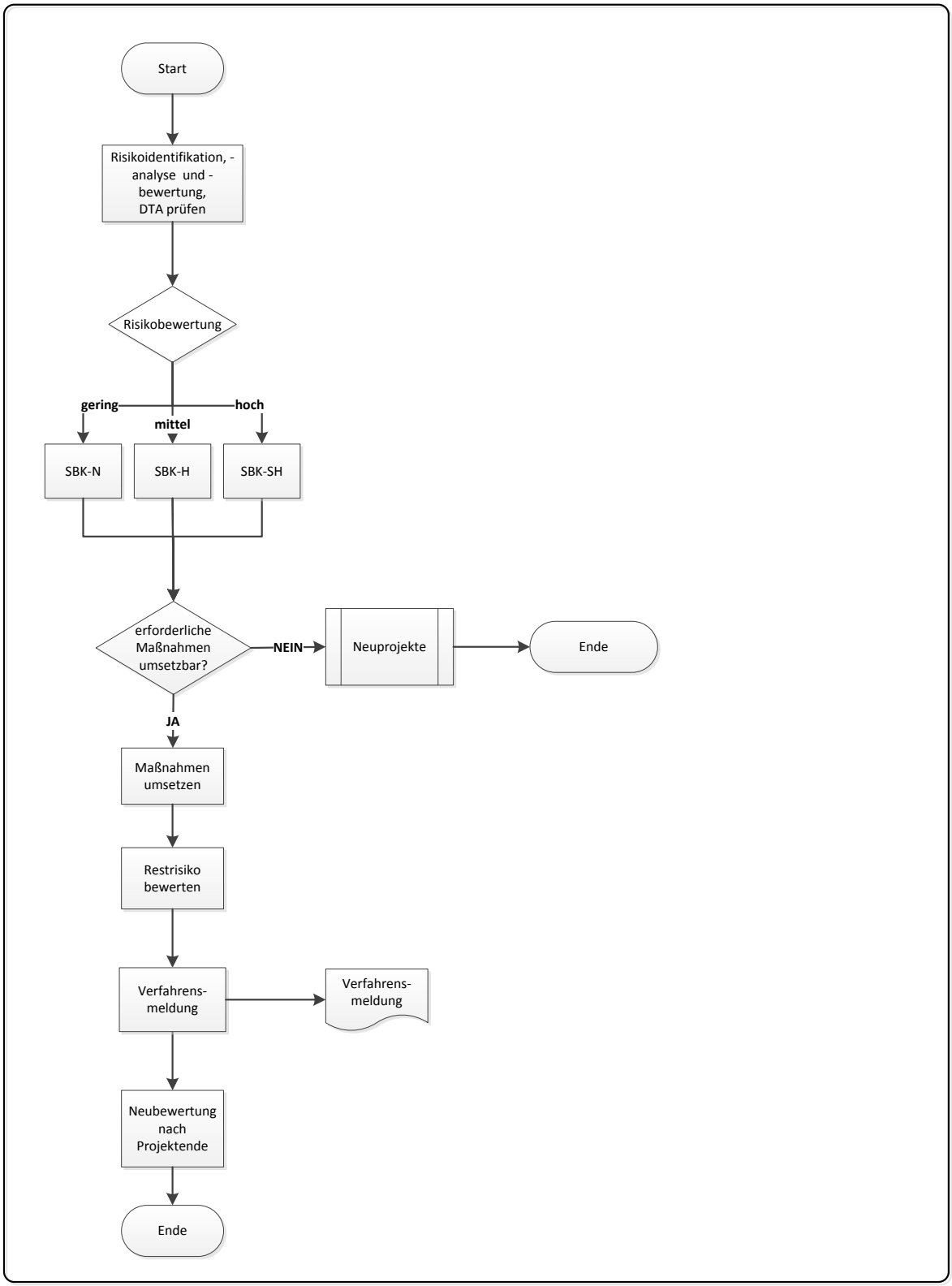

Abbildung 1: Übersichtsdiagramm Bestandsprojekte

2.3.2. Neue Projekte

Neue Projekte sind in diesem Zusammenhang Projekte, die zum Zeitpunkt des Inkrafttretens des Rahmendatenschutzkonzeptes geplant, aber noch nicht durchgeführt werden.

Im Einzelnen sind folgende Schritte durchzuführen:

1. Es ist zu prüfen, ob ein DTA (z.B. Vertraulichkeitsverpflichtung) vorliegt (falls ja, ist dieses zu prüfen). Zudem ist eine Analyse und Klassifizierung der Daten vorzunehmen.
2. Wenn es die wissenschaftliche Aufgabe erlaubt, sind die Daten in kritische und weniger kritische Datenpools aufzuteilen.
3. Die einzelnen Datenpools und geplanten Verarbeitungsschritte sind einer Risikoanalyse zu unterziehen.
4. Die Risikoanalyse führt zu einer Einordnung in eine Schutzbedarfsklasse. Diese kann für die unterschiedlichen Datenpools verschieden sein. Dabei werden Datenpools, die personenidentifizierende Daten (IDAT) enthalten, immer in SBK-SH eingestuft.
5. Aus der ermittelten Schutzbedarfsklasse ergeben sich die Schutzmaßnahmen, die umzusetzen sind.
6. Unter Berücksichtigung der finalen Schutzbedarfsklassen ist in einer abschließenden Risikoanalyse das Restrisiko zu bewerten.
7. Für das Projekt ist eine Verfahrensmeldung bei dem Datenschutzbeauftragten des DKFZ einzureichen.
8. Wenn die Daten aus rechtlichen oder projektspezifischen Gründen über das Projektende hinaus aufbewahrt werden müssen, ist für diesen Aufbewahrungszeitraum eine erneute Risikoanalyse durchzuführen.

Die Verfahrensweise bei neuen Projekten ist in Abbildung 2 grafisch aufbereitet.

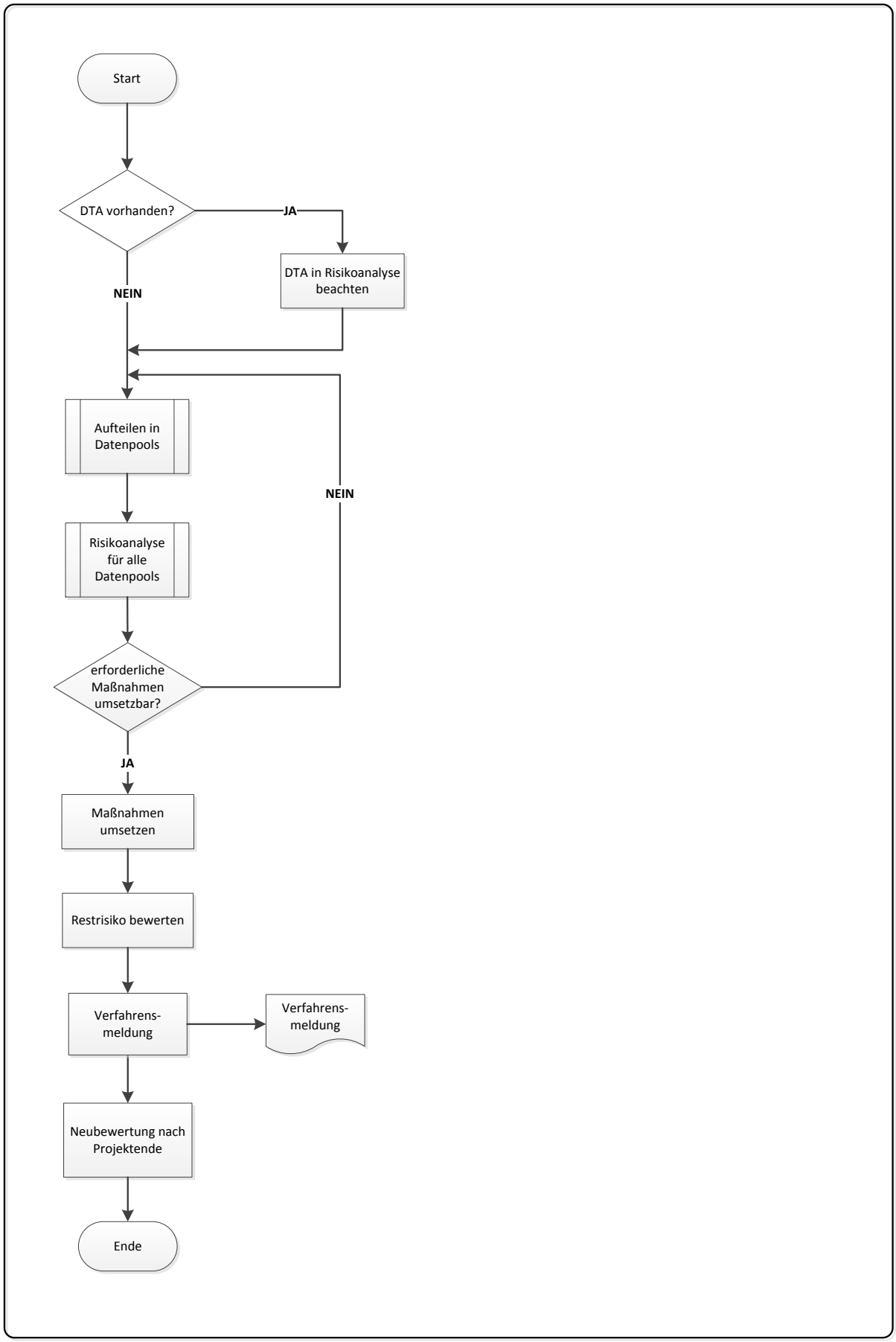

Abbildung 2: Übersichtsdiagramm für neue Projekte

2.3.3. Aufteilung in Datenpools

Um dem grundlegenden Gebot des Datenschutzrechtes zur Datenvermeidung bzw. Datensparsamkeit Folge zu leisten, sind folgende Schritte durchzuführen:

1. Es ist festzustellen, ob in den zu verarbeitenden Daten IDAT enthalten sind.
2. Wenn IDAT enthalten sind, ist zu prüfen, ob diese Angaben zur Erreichung des Projektzieles benötigt werden, oder ob die Daten auch in anonymisierter bzw. pseudonymisierter Form bearbeitet werden können.
3. Falls IDAT benötigt werden, ist zu prüfen,
   - ob der Umfang der erforderlichen personenidentifizierenden Daten reduziert werden kann,
   - ob der Personenbezug über den gesamten Verarbeitungsablauf erhalten bleiben muss und, wenn nicht, wie lange der Personenbezug erhalten bleiben muss.
4. Wenn das Projektziel auch mit anonymisierten Daten erreicht werden kann, so sind die identifizierenden Daten zum frühestmöglichen Zeitpunkt zu entfernen. Dieser Vorrang wird als de-identifizierend bezeichnet, da die Daten keinen Bezug zu einer Person aufweisen.
5. Wenn das Projektziel auch mit pseudonymisierten Daten erreicht werden kann, mit anonymisierten Daten jedoch nicht, sind die identifizierenden Daten zum frühestmöglichen Zeitpunkt durch ein Pseudonym (PSN), das z.B. durch den zentralen oder einen anderen Pseudonymisierungsdienst (siehe Kapitel 3.3.6) oder durch den Projektpartner erzeugt wird, zu ersetzen, so dass kein direkter Bezug zu einer bestimmten Person möglich ist.

Nach dieser Einteilung entstehen vier mögliche Datenpools:

IDAT + MDAT:	personenidentifizierende Daten (mit den zugehörigen medizinischen Daten
PSN + MDAT:	mit einem Pseudonym versehene medizinischen Daten
IDAT + PSN:	die Zuordnung der pseudonymisierten Daten zu den identifizierenden Daten
MDAT:	medizinische Daten, d.h. de-identifizierten Daten ohne Bezug zu einer Person

Die Aufteilung in die verschiedenen Datenpools ist in Abbildung 3 dargestellt.

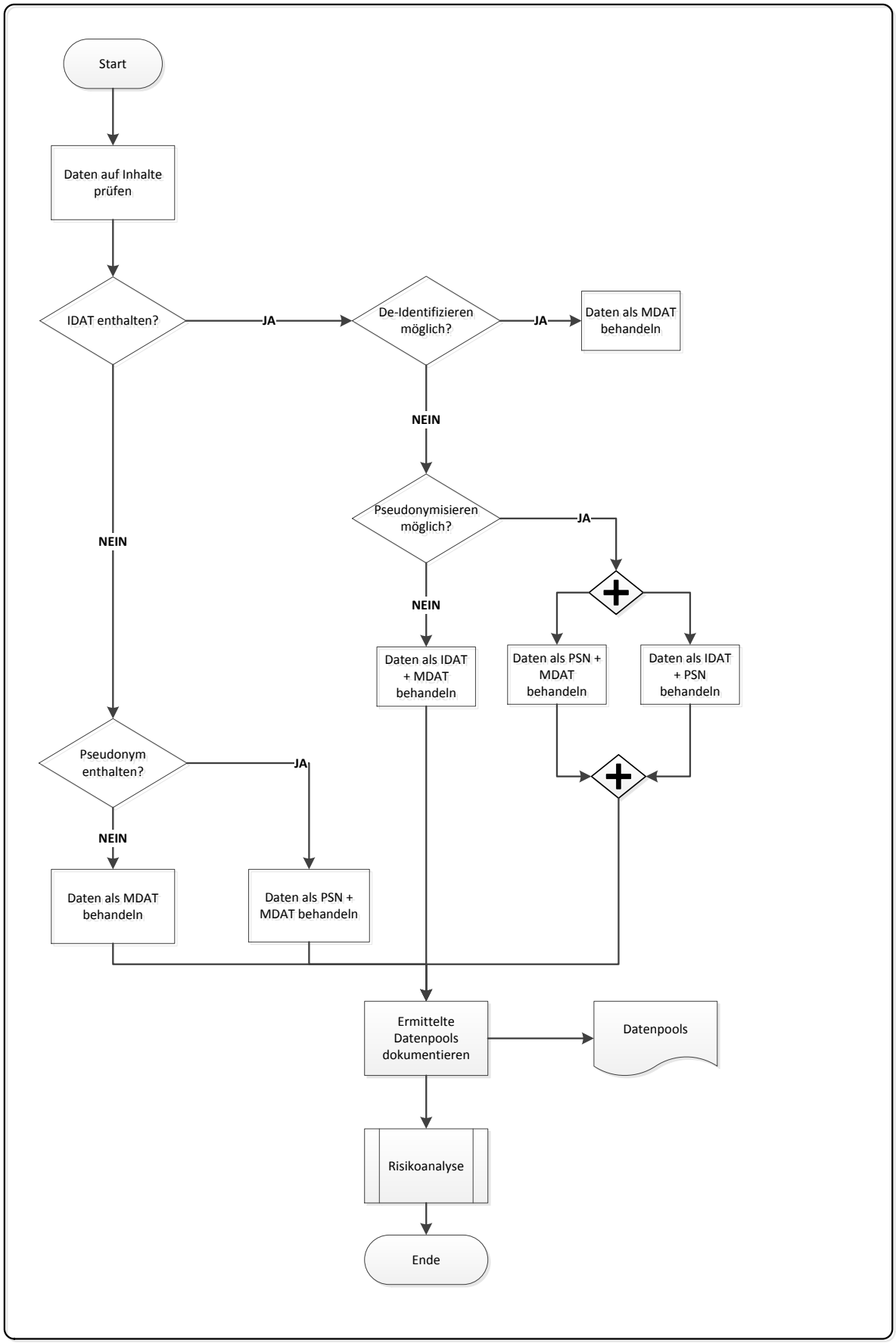

Abbildung 3: Übersichtsdiagramm zur Aufteilung in Datenpools

2.4. Risikoanalyse

Die Risikoanalyse wird zur Identifikation und Bewertung von Risiken eingesetzt, damit mögliche negative Ereignisse (=Risiken) durch das Ergreifen von Schutzmaßnahmen vermieden oder reduziert werden können. Dabei wird das Risiko allgemein als Produkt aus Eintrittswahrscheinlichkeit eines unerwünschten Ereignisses und der Schadensauswirkung als Konsequenz aus dem Ereignis angesehen.
In den folgenden Kapiteln werden die einzelnen Schritte zur Ermittlung des Risikos beschrieben. Das Ergebnis der Risikoanalyse wird Bestandteil der Verfahrensmeldung und an den Datenschutzbeauftragten gemeldet.

2.4.1. Risikoereignis

Ein Risikoereignis bezeichnet ein einzelnes Ereignis, welches bei seinem Eintreten ein Projekt zum Positiven oder Negativen beeinflussen kann.

Es müssen mindestens folgende Risikoereignisse (RE) einzeln betrachtet werden:

RE1: Die Daten gelangen in die Hände von Unbefugten bzw. werden an Unbefugte weitergegeben.
RE2: Pseudonymisierte oder anonymisierte Daten werden re-identifiziert, d.h. sie werden unbefugt wieder der Person zugeordnet.
RE3: Die Daten werden manipuliert, d.h. sie werden verfälscht, vertauscht oder durch technische Probleme fehlerhaft.
RE4: Die Daten werden unbefugt gelöscht.
RE5: Vorgaben aus einem Data Transfer Agreement / einer Einwilligungserklärung / oder sonstige rechtliche Vorgaben (z.B. Aufbewahrungs- und Löschfristen, Zweckbindung, Datensparsamkeit, fehlende Transparenz für den Betroffenen) werden nicht erfüllt.

Zu jedem Risikoereignis werden die Eintrittswahrscheinlichkeit bei der beabsichtigten Arbeitsweise und die Schadensauswirkung bei Eintritt des Ereignisses benannt und bewertet.

2.4.2. Schadenseintrittswahrscheinlichkeiten

Die Eintrittswahrscheinlichkeit ist eine quantitative oder qualitative Angabe über die Wahrscheinlichkeit, mit der ein Risikoereignis innerhalb eines bestimmten Zeitraums eintritt. In Anlehnung an das DKFZ Risikomanagement werden drei Stufen der Schadenseintrittswahrscheinlichkeit festgelegt, siehe Tabelle 1. Die Definitionen sollen zur Orientierung dienen und können im Einzelfall angepasst werden. Kriterien zur Anpassung dieser Definitionen können beispielsweise die Projektinhalte, die Größe und Zusammensetzung eines Projektteams, also der zugriffsberechtigten Personen sein.

Tabelle 1: Einteilung der Schadenseintrittswahrscheinlichkeiten

Schadenseintrittswahrscheinlichkeit	Beschreibung
unwahrscheinlich	Der Eintritt eines Schadens soll als „unwahrscheinlich“ gelten, wenn die Wahrscheinlichkeit für den Eintritt des Schadens bei weniger als 1% während der Projektlaufzeit bzw. Aufbewahrungsfrist liegt.
möglich	Als „möglich“ soll gelten, wenn die Wahrscheinlichkeit für den Eintritt des Schadens bei weniger als 10% während der Projektlaufzeit bzw. Aufbewahrungsfrist liegt.
wahrscheinlich	Als „wahrscheinlich“ soll gelten, wenn die Wahrscheinlichkeit für den Eintritt des Schadens bei mindestens 10% während der Projektlaufzeit bzw. Aufbewahrungsfrist liegt.

2.4.3. Schadensauswirkungen

Unter der Annahme, dass der Schadensfall eingetreten ist, gilt es, die Auswirkung des Schadens in Schweregrade einzuteilen, siehe Tabelle 2. Der Schweregrad ist gegeben, wenn einer der unter „Beschreibung“ angegebenen Punkte eintritt, wobei die höchste Schadensauswirkung zählt.

Tabelle 2: Einteilung der Schadensauswirkung

Schadensauswirkung	Beschreibung
unbedeutend	• Verstöße gegen Vorschriften und Gesetze haben geringfügige Konsequenzen. • Bei Schadensfällen bzgl. personenbezogener Daten kann der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen unwesentlich beeinträchtigt werden, es ist keine Beeinträchtigung der persönlichen Unversehrtheit denkbar. • Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten (Grundwert Vertraulichkeit). • Die Beeinträchtigung der Aufgabenerfüllung würde von den DKFZ-Beschäftigten als tolerabel eingeschätzt werden (Grundwert Verfügbarkeit) • Der wirtschaftliche Schaden bleibt für die Institution gering (<10.000 €).
moderat	• Verstöße gegen Vorschriften und Gesetze haben erhebliche Konsequenzen. • Bei Schadensfällen bzgl. personenbezogener Daten kann der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden, eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.

	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. • Die Beeinträchtigung der Aufgabenerfüllung würde von einzelnen DKFZ-Beschäftigten als nicht tolerabel eingeschätzt. • Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend (10 – 100 T€).
wesentlich	• Verstöße gegen Vorschriften und Gesetze haben schwerwiegende Konsequenzen. • Bei Schadensfällen bzgl. personenbezogener Daten ist eine Gefahr für Leib und Leben oder eine Beeinträchtigung der persönlichen Freiheit des Betroffenen gegeben. • Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar. • Die Beeinträchtigung der Aufgabenerfüllung würde von allen DKFZ-Beschäftigten als nicht tolerabel eingeschätzt. • Der finanzielle Schaden ist für die Institution existenzbedrohend (>100 T€)

2.4.4. Risikomaßzahl

Für die Berechnung des Risikos werden sowohl den Eintrittswahrscheinlichkeiten als auch den Schadensauswirkungen Maßzahlen zugeordnet:

Eintrittswahrscheinlichkeit „unwahrscheinlich“ = 1
Eintrittswahrscheinlichkeit „möglich“ = 2
Eintrittswahrscheinlichkeit „wahrscheinlich“ = 3

Schadensauswirkung „unbedeutend“ = 2
Schadensauswirkung „moderat“ = 4
Schadensauswirkung „wesentlich“ = 6

Mit Hilfe der Risikomatrix wird die Risikomaßzahl als Produkt aus Eintrittswahrscheinlichkeit und Schadenauswirkung gebildet.

Tabelle 3: Ermittlung der Risikomaßzahl

Eintritts-wahrscheinlichkeit	**Schadensauswirkung**		
	unbedeutend (=2)	**moderat (=4)**	**wesentlich (=6)**
Unwahrscheinlich (=1)	**2**	**4**	**6**
Möglich (=2)	**4**	**8**	**12**
Wahrscheinlich (=3)	**6**	**12**	**18**

Aus der berechneten Risikomaßzahl werden drei Risikokategorien erzeugt:

2 - 4: geringes Risiko
6 - 12: mittleres Risiko
> 12: hohes Risiko

Zur besseren Lesbarkeit sind diese Risikokategorien in Tabelle 3 farblich gekennzeichnet.

Die Risikoanalyse ist für jeden Datenpool und für jedes der vorgenannten Risikoereignisse durchzuführen. Es gilt das Maximumprinzip: Die höchste ermittelte Risikokategorie ist für die Einstufung des Datenpools in eine Schutzbedarfsklasse heranzuziehen. Die Einstufung in die Schutzbedarfsklasse ist in Abbildung 4 schematisch dargestellt:

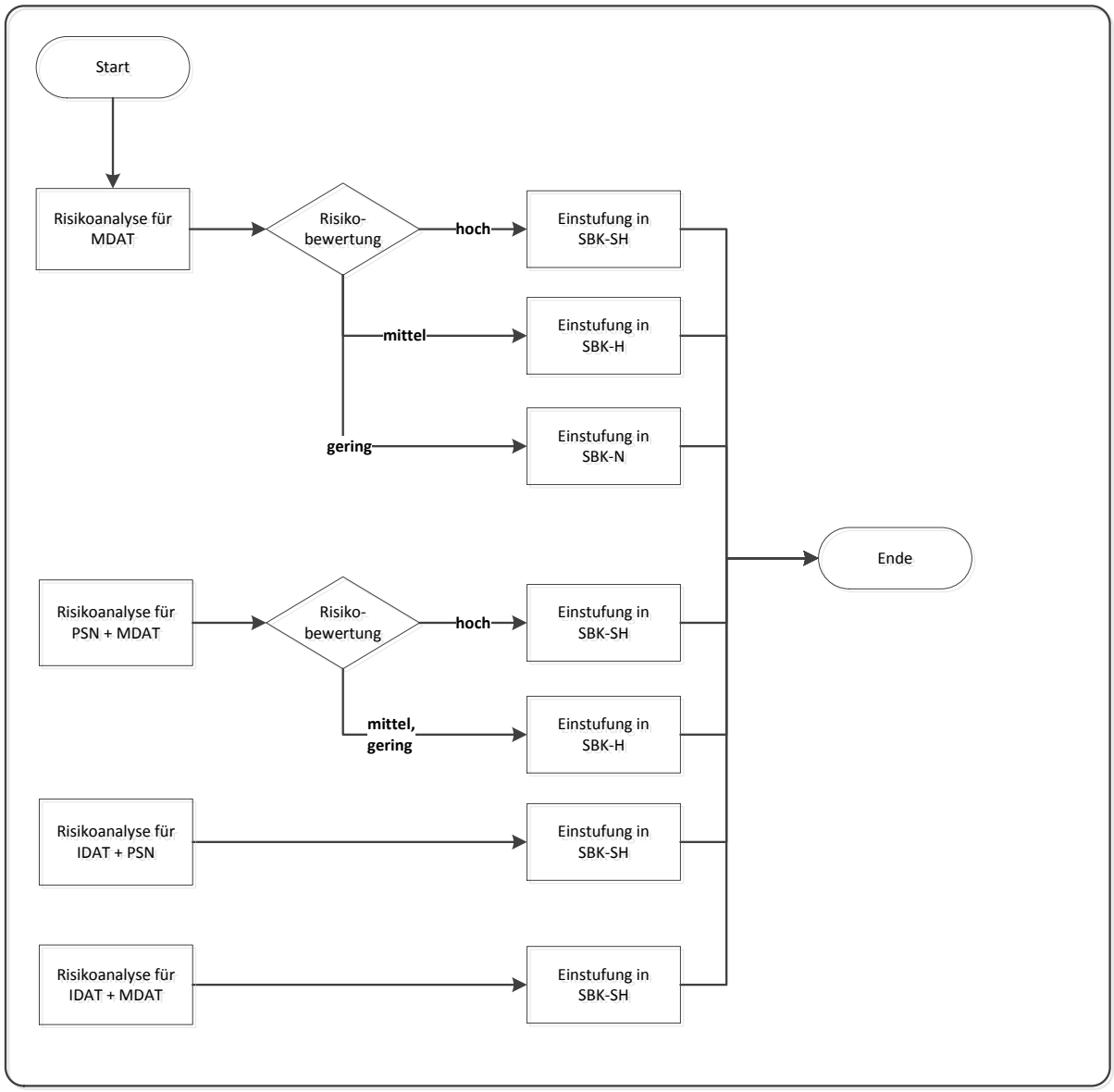

Abbildung 4: Übersichtsdiagramm zur Risikoanalyse

2.4.5. Übersichtstabelle Risikoanalyse

Für jeden Datenpool ist als Ergebnis der Analyse die folgende Tabelle auszufüllen:

Tabelle 4: Übersichtstabelle Risikoanalyse

Datenpool <Name>	Risiko-Ursache	Schadens-auswirkung (Kap. 2.4.3.)	Eintrittswahr-scheinlichkeit (Kap. 2.4.2.)	Risikomaßzahl (Kap. 2.4.4.) und ermittelte SBK	Maßnahmen der Schutz-bedarfsklasse	Schadensauswirkung Restrisiko	Eintrittswahr-scheinlichkeit Restrisiko	Risikomaßzahl Restrisiko
Risiko-ereignis 1		Wählen Sie ein Element aus.	Wählen Sie ein Element aus.			Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
Risiko-ereignis 2								
Risiko-ereignis 3								
Risiko-ereignis 4								
Risiko-ereignis 5								

3. Ableitung der Schutzmaßnahmen aus den Schutzbedarfsklassen

§ 9 Absatz 3 LDSG-BW sieht bei der Verarbeitung personenbezogener Daten vor, geeignete Maßnahmen zu treffen, um die Vorschriften des Datenschutzes anhand 11 definierter Datenschutzkontrollmaßnahmen zu erfüllen.
Die zu ergreifenden Schutzmaßnahmen werden im Gesetz nicht konkret beschrieben, da ihre Eignung vom jeweiligen Anwendungsfall und dem Schutzbedarf der personenbezogenen Daten abhängig ist und die technischen Maßnahmen einem permanenten Wandel unterliegen.
In den folgenden Tabellen zu den einzelnen Kontrollanforderungen werden die möglichen Maßnahmen den verpflichtend umzusetzenden Maßnahmen gegenübergestellt. Maßnahmen, die das DKFZ zusätzlich umsetzt bzw. aus den Vorschriften des Datenschutzes extrahiert bzw. konkretisiert, sind als „weitere Maßnahmen“ aufgeführt. Dabei bedeutet „**+**“ die Maßnahme wird umgesetzt, „**o**“ bedeutet, die entsprechende Maßnahme wird nicht zwingend umgesetzt und „**-**“ bedeutet, die Maßnahme darf nicht durchgeführt werden. Die im Anschluss an die jeweilige Tabelle folgende Beschreibung konkretisiert die im DKFZ umzusetzenden Maßnahmen.

3.1. Datenschutzkontrollen

3.1.1. Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte physikalischen Zutritt zu Datenverarbeitungsanlagen haben, mit denen personenbezogene Daten verarbeitet werden. Die Größe der Datenverarbeitungsanlage ist dabei unerheblich. Unter Zutritt ist die Annäherung an DV-Anlagen mit der Möglichkeit zu verstehen, auf diese einzuwirken und/oder von Daten Kenntnis nehmen zu können. Dies betrifft Serversysteme, Netzwerk und Endgeräte.

Tabelle 5: Maßnahmen zur Zutrittskontrolle

Mögliche Maßnahmen	**Umzusetzende Maßnahmen**		
	SBK SH	**SBK H**	**SBK N**
technische Maßnahmen:			
Einbruchmeldeanalage	+	+	o
Absicherung von Gebäudeschächten	+	+	o
Automatisches Zugangskontrollsystem	+	+	o
Biometrische Zugangssperren	o	o	o
Chipkarten-/Transponder-Schließsystem	+	+	+
Lichtschranken / Bewegungsmelder	+	+	o
Manuelles Schließsystem	+	+	+
Schließsystem mit Codesperre	+	+	o
Sicherheitsschlösser	+	+	+
Videoüberwachung der Zugänge	+	+	o

organisatorische / personelle Maßnahmen:			
Personenkontrolle beim Pförtner / Empfang	o	o	o
Protokollierung der Besucher / Besucherbuch	+	+	o
Schlüsselregelung / Schlüsselbuch	+	+	+
Sorgfältige Auswahl von Sicherheitspersonal	+	+	+
Tragepflicht von Beschäftigten- / Gästeausweisen	o	o	o
Weitere Maßnahmen:			
Liste der zutrittsberechtigten Personen zu den Netzwerkverteilerräumen	+	+	+
Arbeitsplätze in nicht öffentlich-zugänglichen Räumen	+	+	o
Absicherung der Arbeitsplätze, damit nur Befugte Zugang haben (z.B. nur Arbeitsplätze aus dem DKFZ-Netz)	+	+	+

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung

Die beschriebenen technischen Maßnahmen lassen sich sinnvollerweise nur in Data Centern für den Betrieb der Server umsetzen, da hier durch die dauernde Speicherung auch das wesentliche Risiko für einen Schadensvorfall besteht. Der Nachweis der umgesetzten Maßnahmen ist bevorzugt durch eine entsprechende Zertifizierung zu erbringen. Das DKFZ präferiert das Trusted Site Infrastructure-Zertifikat (TSI) des TÜV-IT, Level 1, und für den Bereich „Sicherheitssysteme und –organisation“ zusätzlich den Level 2. Level 1 entspricht den Infrastrukturanforderungen der BSI Grundschutzkataloge im Baustein „Rechenzentrum“. Das TSI-Zertifikat ist in Deutschland allgemein anerkannt.

Die beschriebenen Levels des TSI-Zertifikats bestätigen die Umsetzung der oben aufgeführten möglichen Maßnahmen bis auf die zurzeit technisch noch nicht ausgereiften biometrischen Zugangssperren, die Chipkarten- oder Transponder-Schließsysteme und die Videoüberwachung. Die beiden letzten Maßnahmen werden im DKFZ zusätzlich umgesetzt. Ebenso sind die Kontrolle der zutrittsberechtigten Personen beim Pförtner, das Protokollieren der Besucher oder das Tragen von Beschäftigen- / Gästeausweisen keine Kriterien zum Erreichen des TSI-Zertifikats und werden im DKFZ auch nicht umgesetzt.

Zur Schlüsselregelung für den Zutritt zu den zentralen Data Centern gibt es ein abgesprochenes Verfahren mit dem Datenschutzbeauftragten.

Die Betreiberverantwortung für zentrale Data Center und das Netzwerk im DKFZ hat die IT Core Facility (ITCF). Sollen die Server und Speichersysteme in dezentralen Data Centern betrieben werden, sind die Sicherheitsstandards entsprechend zu prüfen und ggfs. anzupassen.

Die Netzwerk-Verteilerräume sind einfacher abzusichern, da nur wenig Personal Zutritt dazu benötigt. Hier ist zentral eine Liste der Zutrittsberechtigen zu pflegen.

Im Allgemeinen ist im Büro-/Laborumfeld jeder Arbeitsplatz so zu sichern, dass nur Befugte Zugang dazu haben (s.a. DKFZ Nutzungsordnung Informationstechnologie, Kap. 4.1 Zugangsschutz).

Zusammenfassung
Die Daten aller Schutzbedarfsklassen dürfen grundsätzlich nur an Orten mit adäquaten Zutrittskontrollen wie oben beschrieben gespeichert und verarbeitet werden. Dies betrifft insbesondere die Orte der Serversysteme und der Netzwerkverteiler. Zusätzlich gilt für die Endgeräte der SBK-H und SBK-SH, dass sie nicht in öffentlich zugänglichen Bereichen stehen dürfen. D.h. die Räume sind abzuschließen, wenn kein Mitarbeiter sich darin befindet.

3.1.2. Datenträgerkontrolle

Ziel der Datenträgerkontrolle ist es, mit Hilfe geeigneter Verfahren zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Art des Datenträgers spielt dabei keine Rolle.

Tabelle 6: Maßnahmen zur Datenträgerkontrolle

Mögliche Maßnahmen:	**Umzusetzende Maßnahme**		
	SBK-SH	**SBK-H**	**SBK-N**
technische Maßnahmen:			
Absicherung der Bereiche, in denen Datenträger aufbewahrt werden (Datenträgerarchiv)	+	+	+
Aufbewahrung in so genannten Data Safes	-	-	-
Maschinelle Datenträgerverwaltung	+	+	+
Maßnahmen gegen unbefugtes Entfernen von Datenträgern	+	+	+
Kopierkontrolle	o	o	o
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	+	+	o
Softwareverriegelung des Bildschirmes bei längerem Inaktivsein des Benutzers (aus: Speicherkontrolle)	o	o	o
Verwendung des Schreibschutzes bei Datenträgern (siehe: „Speicherkontrolle“)	o	o	o
Trennung des Test- und Produktionsbetriebes (siehe: „Speicherkontrolle“)	+	+	o
organisatorische / personelle Maßnahmen:			
Protokollierung der autorisierten Weitergabe von Datenträgern	+	+	o
weitere Maßnahmen:			
Datenträger in Servern in zentralen Data Centern, Verschlüsselung (siehe „Speicherkontrolle“)	+	o	o
Datenträger in zentralen Servern, unverschlüsselt	-	-	o
Datenträger in Abteilungsservern in dezentralen Data Centern und Workstations, Verschlüsselung (siehe „Speicherkontrolle“)	-	+	o
Datenträger in Abteilungsservern und Workstations, unverschlüsselt	-	-	o

Mobile Datenträger, Verschlüsselung (siehe „Speicherkontrolle“)	-	-	+
Kontrolliertes und protokolliertes Löschen der Daten	+	+	o

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung

Daten der SBK-SH sind ausschließlich auf Festplatten und Bändern von Servern in zentralen, d.h. von der ITCF oder einer Fachabteilung betreuten Data Centern zu speichern. Die Daten müssen auf den Datenträgern verschlüsselt abgelegt werden. Wenn das Medium diesen Service noch nicht bietet, sind die Daten durch den Benutzer zu verschlüsseln. Wenn beides nicht möglich ist (z.B. weil die Datenmenge zu groß ist), ist in der Verfahrensmeldung darauf hinzuweisen und die Mitarbeiter sind explizit auf den besonders sorgsamen Umgang mit den Daten zu verpflichten (s.a. Benutzerkontrolle). Die Datenträger werden nur von autorisiertem Personal der ITCF gewartet. Die Daten dürfen nicht auf andere Medien wie USB-Festplatten oder Workstations im Laborumfeld etc. kopiert werden.

Für Daten der SBK-H sind Datenträger in Servern in zentralen Data Centern oder in Abteilungsservern eines dezentralen Data Centers zu nutzen. Sie dürfen zum Zwecke der Verarbeitung zeitlich befristet auf Workstations zwischengespeichert werden. Die Daten müssen verschlüsselt abgelegt werden. Es gelten hier die Ausführungen zu SBK-SH. Zum Löschen/Archivieren der Daten gelten ebenfalls die Ausführungen zu SBK-SH. Für das komplette Löschen auf Workstations ist der Benutzer selbst verantwortlich. Es ist darauf zu achten, dass die Daten nicht nur in den Papierkorb verschoben werden, eine Wiederherstellung auf Betriebssystemebene ist verboten.

Daten der SBK-N sollen auf Datenträgern in Servern eines Data Centers (zentral oder dezentral) gespeichert werden. Sie dürfen zum Zwecke der Verarbeitung auf Workstations zwischengespeichert oder zum Transport als Kopie auf mobilen Datenträgern verschlüsselt gespeichert werden.

Allgemein gilt bei Daten aller SBKs, dass bei Anforderung durch Kooperationspartner (z.B. Entzug des Einverständnisses des Betroffenen oder nach Ablauf der gewährten Nutzungszeit) das Löschen der Daten durch die Benutzer in Absprache mit der ITCF durchzuführen (s. Zentraler Datenlöschdienst) und zu protokollieren ist. Eventuelle Archivierungspflichten sind zu beachten und hierfür der zentrale Archivierungsdienst zu nutzen. Ansonsten sind die Daten durch den Benutzer mit den üblichen Methoden zu löschen. Es ist zu gewährleisten, dass die Daten in den Datensicherungssystemen nach einem definierten Zeitraum (üblicherweise max. 100 Tage) ebenfalls automatisch gelöscht werden.

Zusammenfassung

Daten aller Schutzbedarfsklassen sollen grundsätzlich nur auf Datenträgern von Servern in Data Centern gespeichert werden. Zum Zwecke der Verarbeitung dürfen Daten der SBK-H und SBK-N temporär – Im Falle von SBK-H verschlüsselt - auf Datenträger in Workstations gespeichert werden.

3.1.3. Speicherkontrolle

Ziel der Speicherkontrolle ist es, mit geeigneten Maßnahmen sicherzustellen, dass personenbezogene Daten nur befugt gespeichert und gespeicherte personenbezogene Daten nur befugt zur Kenntnis genommen, verändert oder gelöscht werden können. Die

Speicherung bezieht sich sowohl auf eine Aufnahme von Daten in den Hauptspeicher einer IT-Anlage als auch auf Datenträger (Festplatten, CD, DVD etc.).

Die Maßnahmen zur Speicherkontrolle werden unter Datenträgerkontrolle, Benutzerkontrolle und Zugriffskontrolle mit abgedeckt.

Mögliche technische Maßnahmen:

- Einsatz von Mitteln zur Authentifikation und Autorisation der Benutzer (siehe Benutzerkontrolle)
- Einführung einer revisionssicheren Zugriffsberechtigungsverwaltung (Active Directory) (siehe Zugriffskontrolle)
- Softwareverriegelung des Bildschirmes bei längerem Inaktivsein des Benutzers (siehe Datenträgerkontrolle)
- Verwendung des Schreibschutzes bei Datenträgern (siehe Datenträgerkontrolle)
- Trennung des Test- und Produktionsbetriebes (siehe Datenträgerkontrolle)
- Kontrolle der System- und User-Aktivitäten (z. B. Protokollierung der Art des Datenzugriffs) (siehe Zugriffskontrolle)
- Datenverschlüsselung (siehe Datenträgerkontrolle)

3.1.4. Benutzerkontrolle

Ziel der Benutzerkontrolle ist es, mit Hilfe geeigneter Authentifizierungs-Maßnahmen zu verhindern, dass unbefugte Personen Datenverarbeitungssysteme, in denen personenbezogene Daten gespeichert werden, mit Hilfe von Einrichtungen der Datenübertragung nutzen können. Unbefugte sind all diejenigen Personen, die keine Berechtigung zur Ausführung dieser Tätigkeit besitzen.

Tabelle 7: Maßnahmen zur Benutzerkontrolle

Mögliche Maßnahmen:	**Umzusetzende Maßnahme**		
	SBK-SH	**SBK-H**	**SBK-N**
technische Maßnahmen:			
Identifikation und Authentifizierung der Benutzer	+	+	+
Vergabe von Zugangscodes	+	+	+
Zugangssicherung zu den Datenverarbeitungsanlagen durch Vorschaltung von Authentisierungsabfragen	+	+	+
organisatorische / personelle Maßnahmen:			
Festlegung der nutzungsberechtigten Personen	+	+	+
Vergabe von Zugangscodes durch eine autorisierte Stelle	+	+	+
weitere Maßnahmen:			
IT-Kooperation mit Externen, Benutzer authentisiert durch externe Institution	+	+	o
IT-Kooperation mit Externen, Benutzer authentisiert durch DKFZ-Mitarbeiter	+	+	+

Schriftliche Verpflichtung der Mitarbeiter/Benutzer, wenn Daten nicht verschlüsselt werden können	+	+	o

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung

Benutzer von Daten der SBK-SH und SBK-H müssen entweder einen gültigen Vertrag mit dem DKFZ haben und sind durch die Personalabteilung zu authentisieren, oder sie sind als Kooperationspartner im Rahmen einer IT-Kooperation von ihrer Institution zu authentisieren. Werden Daten der SBK-SH verarbeitet, die aus oben beschriebenen Gründen (s. Datenträgerkontrolle) nicht verschlüsselt abgelegt werden können, sind die Benutzer explizit und schriftlich auf den sorgsamen Umgang mit diesen Daten zu verpflichten.

Benutzer von Daten der SBK-N können auch DKFZ-Partner sein, die im Rahmen einer IT Kooperation zumindest durch den DKFZ-Verantwortlichen authentisiert wurden.

Zusammenfassung

Auf Daten aller SBKs können nur Benutzer zugreifen, die sich authentisiert haben.

3.1.5. Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, mit Hilfe von geeigneten Maßnahmen sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Tabelle 8: Maßnahmen zur Zugriffskontrolle

Mögliche Maßnahmen	**Umzusetzende Maßnahmen**		
	SBK SH	**SBK H**	**SBK N**
technische Maßnahmen:			
Anlegen von revisionssicheren Benutzerprofilen	+	+	+
Authentifikation und Autorisation der Benutzer	+	+	+
Maschinelle Überprüfung der Berechtigungen	o	o	o
Einführung zugriffsbeschränkender Maßnahmen (z. B. nur Leseberechtigung)	+	+	o
Zeitliche Begrenzung der Zugriffsmöglichkeiten	+	+	o
Beschränkung der freien Abfragemöglichkeiten von Datenbanken (Query-Sprache)	o	o	o
Benutzerbezogene Protokollierung der Fehl-Zugriffe	+	o	o
organisatorische / personelle Maßnahmen:			
Vergabe und Änderung von Berechtigungen nur mit schriftlichem, vom Vorgesetzten unterzeichneten Antrag	+	+	o
weitere Maßnahmen:			

Protokollieren, wer wann auf die Daten zugegriffen hat (siehe „Speicherkontrolle“)	+	+	o
Protokollieren, was mit den Daten gemacht wurde (siehe „Speicherkontrolle“)	+	o	o
Protokollieren über den zentralen Protokollierungsdienst (siehe „Speicherkontrolle“)	+	+	o

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung
Bei Daten der SBK-SH muss protokolliert werden, wer wann auf die Daten zugegriffen hat und was mit den Daten gemacht wurde (Anlegen, Lesen, Schreiben, Ändern, Kopieren, Löschen). Es sind alle Zugangsversuche, sowohl die erfolgreichen als auch die erfolglosen, zu protokollieren. Der zentrale Protokollierungsdienst ist zu nutzen (siehe Kapitel 3.3.2). Sinnvollerweise können Zugriffe auf Daten der SBK-SH nur in Datenbanken oder anderen Anwendungen (wie z.B. Pipelines) verwaltet werden. Die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer erfolgt ausschließlich auf schriftlichen Antrag, der vom Vorgesetzten unterzeichnet ist. Bei Widerruf der Einwilligung in die Datennutzung seitens des Betroffenen sind dessen personenbezogene Daten, nach Ablauf der gewährten Nutzungszeit sind alle beim bisher berechtigten Nutzer vorhandenen personenbezogenen Daten zu löschen. Die Löschung ist zu protokollieren (s.a. Datenträgerkontrolle)
Für Daten der SBK-H reicht es aus zu protokollieren, wer wann auf die Daten zugegriffen hat. Der zentrale Protokollierungsdienst ist zu nutzen (s.u.).
Für Daten der SBK-N ist eine Protokollierung des Zugriffes nicht erforderlich.
Generell gelten zum Thema Löschen die Ausführungen unter „Datenträgerkontrolle“.

Zusammenfassung
Der Zugriff zu Daten aller SBKs ist nur autorisierten Benutzern möglich. Die Zugriffe auf Daten der SBK-SH und –H müssen mithilfe des zentralen Protokollierungsdienstes protokolliert werden.

3.1.6. Übermittlungskontrolle

Ziel der Übermittlungskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen der Datenübertragung übermittelt werden können. Hier kommt es auf die nach der Verfahrenskonzeption vorgesehene Übermittlung an (auch im Rahmen von automatisierten Abrufverfahren). Die Überprüfung und Feststellung muss nicht dauernd erfolgen, aber sie muss jederzeit möglich sein.

Tabelle 9: Maßnahmen zur Übermittlungskontrolle

Mögliche Maßnahmen:	**Umzusetzende Maßnahmen**		
	SBK-SH	**SBK-H**	**SBK-N**
technische Maßnahmen:			
Dokumentation der Abruf- und Übermittlungsprogramme	+	+	+

Festlegung der Übermittlungswege und der Datenempfänger	+	+	o
Protokollierung der Datenübermittlung	+	+	+
Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können	+	+	o
organisatorische / personelle Maßnahmen:			
Data Transfer Agreement (DTA)	+	+	o
Data Access Committee (DACO)	+	+	o

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung
Daten der SBK-SH und SBK-H dürfen nur aufgrund valider Data Transfer Agreements an benannte Kooperationspartner verschlüsselt in elektronischer Form übermittelt werden. Für Daten der SBK-SH ist zusätzlich ein Votum des Data Access Committee (DACO) notwendig. Die Übermittlung muss durch die Einwilligungserklärung des Betroffenen abgedeckt sein. Es muss protokolliert werden, wer wann welche Daten an welche Zieladresse an welchen Empfänger gesendet hat. Es muss gewährleistet sein, dass die Daten nur dem gewünschten Empfänger zur Verfügung stehen. Der zentrale Protokollierungsdienst ist zu nutzen (s Kap. 3.3.2.)
Die Übermittlung von Daten der SBK-N muss nicht protokolliert werden, es wird aber empfohlen, dies zu tun.

Zusammenfassung
Die Bedingungen unter denen Daten der SBK-SH und SBK-H übermittelt werden dürfen, müssen in den jeweiligen Data Transfer Agreements festgehalten werden. Dazu gehören Anlass und Zweck der Übermittlung, Art und Umfang der zu übermittelnden Daten, Benennung der Empfänger der Daten, Transportweg etc.

3.1.7. Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich die näheren Umstände einer Dateneingabe überprüft und festgestellt werden können. Die Überprüfung und Feststellung sollte nach erfolgter Eingabe anhand von Unterlagen möglich sein. Es sind Fälle denkbar, dass bei bestimmten Eingaben Veranlasser, Grund und Zeitpunkt mitgespeichert oder in einer personenbezogenen Protokolldatei abgespeichert werden.

Mögliche technische Maßnahmen:

- Festlegung von Eingabebefugnissen (Autorisation) (siehe Benutzerkontrolle)
- Protokollierung der Eingaben, Veränderungen und Löschungen (Audit Trail) (siehe Zugriffskontrolle)

Weitere Maßnahmen:

- Einrichtung externer IT-Kooperationen (siehe Benutzerkontrolle)

Die Maßnahmen zur Eingabekontrolle sind unter Benutzerkontrolle und Zugriffskontrolle mit abgedeckt.

3.1.8. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur nach den Weisungen des Auftraggebers verarbeitet werden.

Tabelle 10: Maßnahmen zur Auftragskontrolle

Mögliche Maßnahmen:	**Umzusetzende Maßnahme**		
	SBK-SH	**SBK-H**	**SBK-N**
technische Maßnahmen:			
organisatorische / personelle Maßnahmen:			
Klare Vertragsgestaltung und –ausführung (Data Transfer Agreement). Die Maßnahmen der entsprechenden Schutzbedarfsklassen sind im Vertrag aufzuführen.	+	+	+
Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber	+	+	+
Sorgfältige Auswahl des Auftragnehmers (wenn DKFZ Auftraggeber ist)	+	+	+
Formalisierung der Auftragserteilung	+	+	+
Protokollierung und Kontrolle der ordnungsgemäßen Vertragsausführung	+	+	+
Benennung eines Verantwortlichen auf DKFZ-Seite	+	+	+
Sanktionen bei Vertragsverletzung	+	+	+
weitere Maßnahmen:			
Einrichten einer „externen IT-Kooperation“ (Service der ITCF)	+	+	+

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung

Wenn Daten im Auftrag verarbeitet werden – unerheblich davon, ob das DKFZ Auftraggeber oder Auftragnehmer ist –, wird auf DKFZ-Seite ein Verantwortlicher bestimmt, der für die Umsetzung der speziellen Anforderungen sorgt und einen jährlichen Audit Trail durchführt. Der Verantwortliche muss einen Stellvertreter benennen. Für jede Auftrags-DV ist eine Sharepoint-Projektseite (sog. „externe IT Kooperation“) als Sammelstelle der notwendigen Unterlagen einzurichten. Da diese Verträge, ab einem Beschaffungswert von derzeit 25 T€ (netto), vom Vorstand des DKFZ unterschrieben werden, berichtet der Verantwortliche bei Fragen direkt an Diesen.

Zusammenfassung

Werden personenbezogene Daten im Auftrag verarbeitet, bleibt der Auftraggeber für die Einhaltung der Gesetze und Vorschriften über den Datenschutz verantwortlich. Er hat den Auftragnehmer sorgfältig auszuwählen.
Auftragnehmer müssen sicherstellen, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Unterauftragsverhältnisse unterliegen der Zustimmung des Auftraggebers. Der Auftraggeber hat ein jederzeitiges Kontrollrecht.

3.1.9. Transportkontrolle

Ziel der Transportkontrolle ist es, zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Mögliche technische Maßnahmen:

- Regelungen für die Versandart und Festlegung des Transportweges (siehe Übermittlungskontrolle)
- Sicherung des Übertragungs- und Transportweges (siehe Übermittlungskontrolle)
- Verschlüsselung der Daten (siehe Datenträgerkontrolle)
- Überprüfung aller Daten und Datenträger hinsichtlich Virenbefall (siehe Datenträgerkontrolle)

Mögliche organisatorische Maßnahmen:

- Festlegung der für die Übermittlung oder den Transport Berechtigten (siehe Übermittlungskontrolle)

Die Maßnahmen zur Transportkontrolle sind unter Datenträgerkontrolle und Übermittlungskontrolle beschrieben.
Der Transport in nicht-elektronischer Form ist ein Sonderfall und muss nur bei Daten der SBK-SH betrachtet werden. Hier ist ein Einschreiben mit persönlicher Empfängerbestätigung oder ein gleichwertiger Übermittlungsweg notwendig.

3.1.10. Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen, also zuverlässig zu sichern und zu archivieren.

Tabelle 11: Maßnahmen zur Verfügbarkeitskontrolle

Mögliche Maßnahmen:	**Umzusetzende Maßnahme**		
	SBK-SH	**SBK-H**	**SBK-N**
technische Maßnahmen:			
Backup	+	+	+
Archivierung	+	+	+

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung
Die ITCF biete den Service „Datensicherung (Backup/Archiv)“ mit Magnetbändern an. Der Teilservice „Backup“ dient zum Schutz vor Defekt von Festplatten. Wenn Daten auf Festplatten gelöscht werden, werden sie auch nach einer festdefinierten Zeit (in der

Regel max. 100 Tage) aus dem Backup-System gelöscht. Um Daten beständig auf Band zu sichern ist der Service „Archiv“ anzuwenden.
Daten auf zentralen Servern werden automatisch per Backup gesichert und die Sicherung wird von der ITCF überwacht. Für die Sicherung von Daten auf Abteilungsservern, Workstations und Arbeitsplätzen ist der Nutzer selbst verantwortlich.
Der Schutzbedarf der gesicherten oder archivierten Daten ist mindestens ebenso hoch wie der der Originaldaten. Entsprechend sind die Maßnahmen für die gesicherten bzw. archivierten Daten umzusetzen.
Für die Archivierung von Daten ist der Nutzer selbst verantwortlich. Für Publikationen ist es notwendig, die Originaldaten zu sichern, so dass diese Daten archiviert werden müssen.

Zusammenfassung
Daten aller SBKs werden durch die ITCF gesichert, sofern sie auf zentralen Datenträgern abgelegt werden.

3.1.11. Organisationskontrolle

Ziel der Organisationskontrolle ist es, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Gemeint ist damit, dass sich der Datenschutz nicht an die Organisation, sondern die Organisation an den Datenschutz anpassen sollte.

Tabelle 12: Maßnahmen zur Organisationskontrolle

Mögliche Maßnahmen:	**Umzusetzende Maßnahme**		
	SBK-SH	**SBK-H**	**SBK-N**
technische Maßnahmen			
Regelmäßige Datensicherung	+	+	+
organisatorische / personelle Maßnahmen:			
Bestellung eines behördlichen Datenschutzbeauftragten	+	+	+
Funktionstrennung innerhalb der DV-Abteilung, sofern das die Abteilungsgröße erlaubt	+	+	+
Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen	+	+	+
Erlass von Programmierrichtlinien	+	+	o
Vorgaben für die Dokumentation der Programme	+	+	o
Beschäftigtenverpflichtung auf die Vertraulichkeit innerhalb eines Projektes	+	+	o
Erlass von Datenschutzrichtlinien und Dienstanweisungen	+	+	o
Schulung der Beschäftigten	+	+	+
Erstellen eines Notfallkonzepts	+	+	+
Erstellen von Bedienungs- und Benutzeranweisungen	+	+	+
Revisionssichere Benutzerverwaltung	+	+	+
Vorgabe der Regelungen für die Passwortvergabe und -	+	+	+

verwaltung			
Zentrale Beschaffung der Hard- und Software	+	+	+

Legende: **„+“** Maßnahme wird umgesetzt; **„o“** Maßnahme wird nicht zwingend umgesetzt; **„-“** Maßnahme darf nicht durchgeführt werden

Beschreibung
Jeder Beschäftigte verpflichtet sich bei seiner Einstellung im Rahmen seines Arbeitsvertrages u.a. auf die Einhaltung der „Nutzungsordnung Informationstechnologie“ und des EURAT-Kodex. Auf dem Einstellungsantrag muss angekreuzt werden, ob mit personenbezogenen Daten gearbeitet wird. Falls dies der Fall ist, erhält der Beschäftigte eine Schulung durch den Datenschutzbeauftragten mit Verweis auf dieses Rahmendatenschutzkonzept. In der Schulung wird darauf hingewiesen, dass die Verletzung der Verpflichtungen u.U. disziplinarische, arbeits-, zivil- oder strafrechtliche Bedeutung hat (Stichpunkte: Verletzung von Dienstgeheimnissen; Verletzung der ärztlichen Schweigepflicht; Verstoß gegen das Gendiagnostikgesetz oder gegen Datenschutzbestimmungen; Verstoß gegen behördliche Vorgaben einschließlich solche einer Ethikkommission; Verletzung der Pflicht, vor Durchführung einer Studie eine Stellungnahme / ein Votum einer Ethikkommission einzuholen; Verletzung des allgemeinen Persönlichkeitsrechts; Nichteinhaltung von projektspezifischen Verpflichtungen).
In dem Personalverwaltungssystem muss diese Information mitgeführt bzw. bei Änderungen modifiziert werden.
Der Beschäftigte, der mit Daten der SBK-SH und SBK-H arbeitet, muss eine schriftliche projektspezifische Verpflichtung unterschreiben.
Die revisionssichere Benutzerverwaltung wird als zentrale Infrastrukturmaßnahme umgesetzt. Projektspezifische Benutzerverwaltungen sind nicht erlaubt.
Die anderen Punkte obliegen den Fachabteilungen und sind dort umzusetzen.

3.2. Organisatorische Maßnahmen

3.2.1. Regelung der Verantwortlichkeiten

Für die Einhaltung der Vorschriften der IT Sicherheit und des Datenschutzes innerhalb eines wissenschaftlichen Projektes ist der jeweilige Projektleiter verantwortlich. Ebenso muss der Projektleiter von seinem Kooperationspartner die Bestätigung einholen, dass die Daten für eine Bearbeitung im DKFZ freigegeben sind (Einverständniserklärung des Patienten, Ethikvotum, Freigabe durch die Institution des Partners etc.). Für Teilbereiche kann diese Verantwortung delegiert werden. Die Voraussetzungen zur Delegation sind entweder institutionell gegeben, oder sind durch entsprechende Maßnahmen (s. „Instrument“ in der Tabelle) zu schaffen. Teilverantwortung übernehmen die folgenden Einheiten:

Tabelle 13: Übersicht der Verantwortlichkeiten

Bereich	Verantwortlicher	Instrument
Gesamtverantwortung	Projektleiter	Verfahrensmeldung
Überwachung der Datenverarbeitungsprozesse	Datenschutzbeauftragter	Verfahrensverzeichnis
IT-Sicherheit	ITCF	Datacenter, allgemeine Regelungen / Vorschriften
Inhaltliche Datensicherheit	Datenverwalter	Anwendungssystem

Datenherausgabe	Data Access Committee	Data Transfer Agreement
Risikomanagement	Projektleiter	Risikoanalyse
Ordnungsgemäße Durchführung des Projektes	Beschäftigter	Vorgaben, SOP, Verpflichtungserklärung

3.2.2. Beschäftigtenverpflichtungen und –schulungen

Der Datenschutzbeauftragte lädt regelmäßig alle neuen Beschäftigten mit Tätigkeitsumfeld „personenbezogene Daten“ und alle Beschäftigten, deren Tätigkeitsbeschreibung diesbezüglich geändert wurde, verpflichtend zu einer Datenschutz-Schulung ein. Diese Schulung ist bei Gesetzesänderungen aufzufrischen.
In der Verfahrensmeldung sind die Funktionen der zugriffsberechtigten Personen aufzuführen. Nur Beschäftigte, die an einer Datenschutz-Schulung teilgenommen haben, dürfen mit personenbezogenen Daten der SBK-SH arbeiten.
Eine Vorlage für die projektspezifische Vertraulichkeitsverpflichtung der Beschäftigten ist zu erstellen.

3.3. Infrastrukturelle und technische Maßnahmen

3.3.1. Zentrales Identitätsmanagement

Die Identitäten von Nutzern, die auf personenbezogene Daten im DKFZ zugreifen, müssen im Normalfall zentral von der ITCF verwaltet werden. Ausschließlich die ITCF bietet im Haus einen validierten Authentifikationsmechanismus (mit Prozessen zur Identitätserstellung) an. Sollten andere Nutzer auf diese Daten zugreifen, gelten die Maßnahmen aus der Benutzerkontrolle.

3.3.2. Zentraler Protokollierungsdienst

Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten so transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
Um die Anforderungen an die Protokollierung revisionssicher umsetzen zu können, muss ein zentraler Protokollierungsdienst eingerichtet werden. Dieser sollte Log-Datensätze von verschiedenen Quellen mit unterschiedlichen Formaten entgegennehmen können. Dieser Dienst wird von der ITCF betrieben.
Die erzeugten Protokolldaten sind vor dem Zugriff Unbefugter zu schützen und werden den Regelungen im RDSK entsprechend behandelt. Die Protokolldaten sind über den zentralen Datenarchivierungsdienst asymmetrisch verschlüsselt zu archivieren.

3.3.3. Zentraler Datenlöschdienst

Bei verschlüsselten Daten ist es für das rückstandsfreie Löschen ausreichend, zusätzlich zum Löschen der Ursprungsdaten den Schlüssel zu löschen. Damit sind die Daten auch auf den Datensicherungssystemen (Snapshots, Band-Backup) nicht mehr interpretierbar und die normalen Löschverfahren auf diesen Systemen werden verwendet.
Bei nicht-verschlüsselten Daten ist eine geeignete Methode z.B. das mindestens 5-fache Überschreiben mit zufälligen Mustern zu verwenden (z.B. durch wipe, Eraser, Shredit, secure rm u.a.). Sollten Backup-Kopien vorhanden sein (lokal oder auf zentralen

Bandlaufwerken), sind auch diese sukzessive durch überschriebene Versionen zu ersetzen, bis keine verwertbaren Versionen mehr vorhanden sind. Das gilt sowohl für Server als auch für Workstations. Es betrifft auch nicht nur die primären Daten, sondern auch alle davon abgeleiteten Dateien, soweit sie noch personenbezogene Daten enthalten.

3.3.4. Zentraler Backup- und Datenarchivierungsdienst

Die Erfüllung der Grundsätze zur Sicherung guter wissenschaftlicher Praxis sowie die Anforderung, publizierte Datenanalysen auch nachträglich analysieren zu können, erfordern eine langfristige Archivierung der Daten mit definierten Zugriffsregeln. Für Projekte, bei denen das datenhaltende System im DKFZ läuft, ist hierfür der Archivierungsdienst der ITCF zu nutzen. Die Schutzbedarfsklasse der archivierten Daten muss mindestens so hoch sein wie die der Originaldaten.

3.3.5. Revisionssichere Benutzerverwaltung

Alle Änderungen der Rechte (i.d.R. Gruppenzugehörigkeiten) von Benutzern müssen im zentralen Protokollierungsdienst gespeichert werden. Dies ist nur mit einem zentralen Identitätsmanagement möglich.

3.3.6. Zentraler Pseudonymisierungsdienst

Zweck des Pseudonymisierungsdienstes ist es, die für die Forschung genutzten Daten von Patienten und Probanden besonders zu schützen. Üblicherweise werden personenbezogene Daten im DKFZ in pseudonymisierter oder anonymisierter Form von den Kooperationspartnern zur Verfügung gestellt. Ist dies nicht der Fall, müssen die Daten vor der weiteren Bearbeitung pseudonymisiert werden. Zu diesem Zweck soll ein zentraler Pseudonymisierungsdienst eingerichtet werden.

Der Pseudonymisierungsdienst erlaubt berechtigten Benutzern, einem Identifikator aus dem klinischen Umfeld, meist dem im Klinikinformationssystem vergebenen Patientenidentifikator, oder den personenidentifizierenden Daten mittels kryptographischer Verfahren ein Pseudonym zuzuordnen. Die Berechtigung zur Nutzung des Pseudonymisierungsdienstes wird in dem zentralen Active-Directory des DKFZ verwaltet.
Die Überführung der Identitätsdaten in ein Pseudonym erfolgt üblicherweise zweistufig. In einem ersten Schritt werden die Identitätsdaten im Rahmen des Identitätsmanagements unter Verwendung einer Patientenliste in ein Pseudonym erster Stufe (PID) übersetzt. Diese PID dient dem Pseudonymisierungsdienst als Ausgangsdatum zur Generierung des Pseudonyms zweiter Stufe (PSN). Dabei sollte für einen Patienten wiederholt das gleiche Pseudonym generiert werden, so dass eine Korrelation mehrerer Proben eines Patienten möglich ist. Das Einsetzen eines asymmetrischen Verschlüsselungsverfahrens ermöglicht eine Trennung der Aufgaben in Bezug auf Pseudonymisierung und De-Pseudonymisierung.

Der eingesetzte Pseudonymisierungsdienst sollte keine Daten außer dem kryptographischen Schlüssel, der die Zuordnung zwischen PID und PSN darstellt, speichern.

3.3.7. Zentrale Datenverwaltung

Die zentrale Verwaltung von Daten ermöglicht es, die Mechanismen Zentrales Identitätsmanagement, Zentrale Protokollierung, Revisionssichere Benutzerverwaltung, Zentrale Pseudonymisierung nachhaltig zu etablieren. Aus diesem Grund ist eine zentrale Datenverwaltung für humane Genomdaten, humane molekulargenetische Daten, humane Sequenzierungsdaten, humane radiologische Daten und humane epidemiologische Daten sinnvoll.

3.3.8. Life Cycle Management

Für die wissenschaftlichen Projektleiter soll eine Plattform zur Verfügung gestellt werden, mit welcher das Projektmanagement begleitet werden kann. Auf dieser Plattform werden notwendige und hilfreiche Dokumente zur Vorbereitung eines Projektes unter Berücksichtigung der Aspekte des RDSKs zur Verfügung gestellt. Sie bietet auch die Möglichkeit Data Transfer Agreements, Risikoanalysen entsprechend den Regelungen des RDSK, Verfahrensmeldung, Maßnahmen bei Einverständniswiderruf (mit Löschprotokoll) und Projektende zu dokumentieren.

3.3.9. Data Access Committee

Ein Data Access Committee (DACO) entscheidet, falls Daten der Schutzbedarfsklasse „hoch“ und „sehr hoch“ mit anderen Organisationen per DTA ausgetauscht werden. Die Besetzung des Gremiums erfolgt entsprechend der Anwendungsfälle unter Beteiligung der jeweiligen Datenlieferanten.
Insbesondere für Genomsequenzdaten ist das DACO als verpflichtende Instanz vorgesehen, da die Speicherung solcher Daten unter einem "controlled access model" in internationalen Datenbanken ein solches DACO erfordert (z.B. European Genome-Phenome Archive).
Eine weitere Aufgabe des DACO besteht in der Überprüfung der Klassifizierung der Daten eines Projektes durch den Projektleiter. Um dem Interessenkonflikt des Projektleiters entgegenzuwirken, soll das DACO das Ergebnis der vom Projektleiter durchgeführten Risikoanalyse und der daraus resultierenden Einstufung der Daten in eine Schutzbedarfsklasse überprüfen.

4. Glossar und Abkürzungen

AMG	Gesetz über den Verkehr mit Arzneimitteln
BDSG	Bundesdatenschutzgesetz
bDSB	betrieblicher oder behördlicher Datenschutzbeauftragte
Betroffener	im Sinne des Datenschutzgesetzes eine bestimmte oder bestimmbare natürliche Person, die ihre Daten zur Verfügung stellt
BSI	Bundesamt für Sicherheit in der Informationstechnik
DACO	Data Access Committee
Datenpool	eine Sammlung von Daten, die gleichen Kriterien entsprechen, z.B. nur Daten ohne personenidentifizierende Merkmale
DKFZ	Deutsches Krebsforschungszentrum
DKTK	Deutsches Konsortium für translationale Krebsforschung, eines der sechs deutschen Zentren für Gesundheitsforschung
DTA	Data Transfer Agreement
EURAT	Ethische und rechtliche Aspekte der Totalsequenzierung des menschlichen Genoms; vom Marsilius-Kolleg gefördertes Projekt zu normativen Fragen der Totalsequenzierung
IDAT	Identifizierende Daten einer Person, wie z.B. wie Name, Adresse
ITCF	IT Core Facility, Zentrale Einheit für Informationstechnologie am DKFZ
Kooperationspartner	Mitarbeiter von Institutionen, die eine Kooperation mit dem DKFZ eingehen
LDSG	Landesdatenschutzgesetz
MDAT	Medizinische Daten einer Person, wie z.B. Diagnosen, Therapien, Laborwerte
MPG	Gesetz über Medizinprodukte) (Medizinproduktegesetz)
personenidentifizierende Stammdaten	laut TMF-Leitfaden sind personenidentifizierende Attribute: persönliche Namen, geographische Daten, Geburtsdatum, Telefonnummer, Faxnummer, Email-Adresse, Web URLs, Internet-Protokoll-Adressen, Sozialversicherungsnummer, Patienten-Identifikator, Fall-Identifikator, Krankenversicherungsnummer,

	Kontoinformationen, biometrischen Identifikatoren für etablierte Identifikationsverfahren(z.B. Retina-Scans, Fingerabdrücke), Vollgesichtsaufnahmen und vergleichbaren Bilder, eineindeutige Identifikationsnummern oder Kodes, Fahrzeugidentifikatoren, Fahrzeugseriennummern inklusive KFZ-Kennzeichen, Geräte-Identifikatoren und Geräteseriennummern, Zertifikats- und Lizenznummern
PID	Patientenidentifikator
PSN	Pseudonym, ein willkürlich gewähltes Kennzeichen, in welches Identifikationsdaten durch eine Abbildungsvorschrift überführt werden
RDSK	Rahmendatenschutzkonzept DKFZ
revisionssicher	Revisionssicher bedeutet, dass die Daten wieder auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher gespeichert sind.
SBK-N	Schutzbedarfsklasse normal
SBK-H	Schutzbedarfsklasse hoch
SBK-SH	Schutzbedarfsklasse sehr hoch
TMF e.V.	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., Dachorganisation für die medizinische Verbundforschung in Deutschland
TSI	Trusted Site Infrastructure
WiRa	Wissenschaftlicher Rat, ein Organ der Stiftung DKFZ, welches das Kuratorium und den Stiftungsvorstand in wissenschaftlichen Angelegenheiten berät

5. Anhänge

5.1. Rechtsvorschriften

5.1.1. Landesdatenschutzgesetz Baden Württemberg

Verweis auf PDF Dokument: LDSG-BW (Stand 17.12.2015)

5.1.2. § 203 Strafgesetzbuch

Verweis auf https://www.gesetze-im-internet.de/stgb/__203.html (abgerufen am 07.10.2016)

5.1.3. EURAT Kodex

Verweis auf PDF Dokument: Anhang EURAT Kodex.pdf

5.2. Verwendete Literatur

Bei der Erstellung des vorliegenden Rahmendatenschutzkonzeptes dienten neben dem bereits erwähnten Landesdatenschutzgesetz Baden Württemberg (LDSG-BW) folgende Richtlinien als Grundlage:

- IT Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Generisches Datenschutzkonzept der TMF e.V.
- Trusted Site Infrastructure (TSI) – Kriterienkatalog des TÜVIT
- https://www.datenschutz-praxis.de/fachartikel/
- EURAT Kodex
- Risikomanagement DKFZ
- DKFZ Nutzungsordnung Informationstechnologie