

Beschluss



des Gemeinsamen Bundesausschusses über die Abnahme des IQTIG-Datenschutzkonzepts

Vom 16. Mai 2019

Der Gemeinsame Bundesausschuss (G-BA) hat in seiner Sitzung am 16. Mai 2019 beschlossen, das gemäß 8. Kapitel 1. Abschnitt § 4 Absatz 4 VerfO vom Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG) erstellte und von einem unabhängigen Gutachter geprüfte Datenschutzkonzept (**Anlage 1**) abzunehmen

Der Beschluss sowie das Ergebnis der Prüfung und Bewertung des unabhängigen Gutachters (**Anlage 2**) werden auf den Internetseiten des G-BA unter www.g-ba.de veröffentlicht.

Berlin, den 16. Mai 2019

Gemeinsamer Bundesausschuss
gemäß § 91 SGB V
Der Vorsitzende

Prof. Hecken



Institut für Qualitätssicherung und
Transparenz im Gesundheitswesen

IQTIG Datenschutzkonzept v2.4

Stand: 26. Februar 2019

Inhalt

1	Zusammenfassung.....	5
2	Einleitung.....	6
3	Aufgabenstellung und Vorgehensweise.....	6
4	Grundsätzliche Einstellung der Einrichtung zum Datenschutz.....	8
5	Fachlicher und organisatorischer Hintergrund der Datenverarbeitung.....	8
6	Rechtsgrundlagen der Datenverarbeitung.....	9
7	Datenschutzbezogene Anforderungen bezogen auf die Verarbeitungsvorgänge / Verarbeitungstätigkeiten beim IQTIG	10
7.1	Grundsätze der Verarbeitung	10
7.1.1	Zweckbindung	10
7.1.2	Datenminimierung	11
7.1.3	Richtigkeit.....	12
7.1.4	Speicherbegrenzung.....	13
7.1.5	Integrität und Vertraulichkeit	13
7.2	Rechtmäßigkeit der Verarbeitung.....	14
7.3	Datenschutz durch Technikgestaltung.....	15
7.4	Sicherheit der Verarbeitung.....	15
7.5	Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Betroffene.....	15
7.6	Datenschutz-Folgenabschätzung	16
7.7	Beachtung der Betroffenenrechte	16
7.7.1	Transparenz und Modalitäten der Betroffenenrechtsausübung.....	17
7.7.2	Informationspflicht und Auskunft zu personenbezogenen Daten des Betroffenen	17
7.7.3	Berichtigung und Löschung, Datenübertragbarkeit.....	18
7.7.4	Widerspruchsrecht.....	18
7.8	Datenverarbeitung beim Verfahren der sekundären Datennutzung.....	18
7.8.1	Besondere Regelungen zur sekundären Datennutzung.....	18
7.8.2	Anträge zur sekundären Datennutzung durch das IQTIG	19
7.8.3	Anträge auf sekundäre Datennutzung durch Mitarbeiterinnen oder Mitarbeiter	19
7.8.4	Anonymisierung der Qualitätssicherungsdaten für die sekundäre Datennutzung.....	19

8	Akteure und Beteiligte an der Verarbeitung	21
8.1	Verantwortlicher/ Verantwortliche der Datenverarbeitung	21
8.1.1	Verantwortlichkeit der Institutsleitung.....	21
8.1.2	Datenschutzbeauftragter	21
8.1.3	Mitarbeiterinnen- und Mitarbeitersensibilisierung	21
8.1.4	Datenübermittlung.....	22
8.2	Auftragsverarbeiter.....	22
9	Aufbewahrungsfristen im Kontext der Zweckbestimmung	23
10	Konkrete Umsetzung der Anforderungen (Kapitel 7 bis 9) bezogen auf die relevanten Verarbeitungstätigkeiten des IQTIG	24
11	Definitionen, Begriffsbestimmungen und Abkürzungen.....	25
12	Anlagen.....	27

1 Zusammenfassung

Das Datenschutzkonzept versteht sich als Beschreibung der Datenschutzorganisation beim IQTIG. Es umfasst die gesamte Tätigkeit im IQTIG. Es beschreibt die Bedingungen zur Verarbeitung von Daten, die im Zusammenhang mit der Erarbeitung und Durchführung von Verfahren der Qualitätssicherung in der Gesetzlichen Krankenversicherung. Hierzu gehören auch Daten von externen Beteiligten, die das IQTIG bei der Erarbeitung, Durchführung und Weiterentwicklung von Qualitätssicherungsverfahren unterstützen. Des Weiteren gilt das Datenschutzkonzept auch für die Verarbeitung von Daten, die der inneren Organisation des IQTIG gelten, wie z. B. Daten der Mitarbeiterinnen und Mitarbeiter. Schließlich enthält dieses Datenschutzkonzept zusätzliche Anforderungen an die Datenverarbeitung im Rahmen der sekundären Datennutzung, also der Nutzung der bereits für die Qualitätssicherung erhobenen Daten zum Zwecke der wissenschaftlichen Forschung und der Weiterentwicklung der Qualitätssicherung für Dritte. Darüber hinaus bearbeitet das IQTIG auch weitere Aufträge des G-BA wie z. B. die Evaluation von Regelungen zu medizinischen Behandlungsprogrammen oder Methoden (z. B. Evaluation der oKFE-RL). Das Datenschutzkonzept beschreibt daher auch den Umgang mit Daten in diesen Fällen.

Das Anliegen des Datenschutzkonzepts ist es, im Interesse der betroffenen Personen und auch des IQTIG in jeder Phase der Datenverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten. Um dieses Ziel zu erreichen, sind nicht nur gesetzliche Vorschriften zum Schutz personenbezogener Daten einzuhalten, sondern auch geeignete technische und organisatorische Maßnahmen umzusetzen. Alle Beschäftigten müssen sich der Risiken bewusst sein, die mit technischen Systemen und Kommunikationstechnologien verbunden sind, und bei der Verarbeitung personenbezogener Daten die erforderliche Sorgfalt walten lassen. Das Datenschutzkonzept definiert daher für aktuelle und künftige Datenverarbeitungen den Anwendungsbereich und Umfang der für das IQTIG geltenden gesetzlichen Vorgaben zum Datenschutz und zur Datensicherheit und dokumentiert verbindlich die zur Umsetzung dieser Vorgaben getroffenen bzw. noch zu treffenden Maßnahmen.

Inhaltlich legt das IQTIG im Datenschutzkonzept in allgemeiner Form fest, dass und wie die gesetzlichen Anforderungen an den Datenschutz, insbesondere die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO), die Rechtmäßigkeit der Datenverarbeitung (Art. 6 DSGVO), die Wahrung der Informationspflichten und der Betroffenenrechte (Art. 12 ff. DSGVO), der Umgang mit Datenschutzvorfällen (Art. 34 DSGVO) sowie die technischen und organisatorischen Maßnahmen (Art. 25 und Art. 32 DSGVO) umgesetzt werden. Bei den Grundsätzen der Datenverarbeitung berücksichtigt das IQTIG insbesondere die für die Qualitätssicherung und sekundären Datennutzung besonders hervorgehobenen Grundsätze der Zweckbindung und der Datensparsamkeit (§§ 137a Abs. 3, 299 SGB V). Die in Bezug auf die konkreten Datenverarbeitungen getroffenen Maßnahmen ergeben sich nicht zuletzt aus dem Verzeichnis von Verarbeitungstätigkeiten des IQTIG sowie weiteren Referenzdokumenten (s. Anlagen).

Die datenschutzrechtliche Überprüfung der Verfahren zur Qualitätssicherung (QS-Verfahren) ist hingegen nicht Gegenstand des Datenschutzkonzepts. Sie erfolgt durch den Gemeinsamer Bundesausschuss (im Folgenden G-BA). Bevor dieser einen Beschluss zur Einführung neuer Verfahren fasst, ist der Bundesbeauftragten für den Datenschutz und die Informationssicherheit nach § 91 Abs. 5a SGB V durch den G-BA Gelegenheit zur Stellungnahme zu geben.

2 Einleitung

Das IQTIG ist ein wissenschaftliches und unabhängiges Institut, das auf der gesetzlichen Grundlage des § 137a SGB V und im Auftrag des untergesetzlichen Normgebers G-BA Aufgaben im Bereich der Qualitätssicherung und der sekundären Datennutzung im Gesundheitswesen wahrnimmt.

Die gesetzgeberischen Ziele der Qualitätssicherung sind die Schaffung eines bundesweit einheitlichen Niveaus in der medizinischen Versorgung, die Optimierung der Behandlungsprozesse und die Aufbereitung der Qualitätssicherungsberichte für die Verfahrensbeteiligten und die Öffentlichkeit. Wesentlicher Bestandteil des Qualitätssicherungsprozesses ist daher die wissenschaftliche Auswertung vorhandener Datenbestände.

Das IQTIG erhebt und verarbeitet zu diesem Zwecke Daten aus dem deutschen Gesundheitswesen. Unter den Daten befinden sich auch personenbezogene Daten respektive Sozialdaten. In der Folge müssen bei der Organisation und Durchführung der Qualitätssicherung und sekundären Datennutzung die gesetzlichen Bestimmungen zum Datenschutz eingehalten werden (z. B. SGB, DSGVO, BDSG, TKG).

Hieraus ergibt sich eine besondere Verantwortung des IQTIG und seiner Mitarbeiterinnen und Mitarbeiter, bei der Verarbeitung von personenbezogenen Daten höchste Anforderungen an den Datenschutz und die Datensicherheit zu stellen.

Für das IQTIG hat es daher oberste Priorität, personenbezogene Daten sowie die Systeme, die diese Daten verarbeiten, vor Verlust, Zerstörung, Nicht-Verfügbarkeit, Diebstahl, unberechtigten Veränderungen, Informationsabfluss, Verfälschung beweisheblicher Daten und unberechtigten Zugriffen zu schützen.

Des Weiteren verarbeitet das IQTIG auch aus eigener Veranlassung erhobene Daten. Dies sind z. B. Daten von Mitarbeiterinnen und Mitarbeitern, externen Beteiligten in den Gremien des IQTIG oder Daten von Dienstleistern. Auch bei diesen Daten handelt es sich um teilweise sensible personenbezogene Daten, die dem gleichen Schutz unterliegen.

3 Aufgabenstellung und Vorgehensweise

Die Verpflichtung zur Erstellung eines Datenschutzkonzepts folgt mittelbar aus der Europäischen Datenschutz-Grundverordnung. Das IQTIG ist als verantwortliche oder beauftragte Stelle bei al-

len Datenverarbeitungsvorgängen zur Dokumentation und Nachweisbarkeit einer datenschutzkonformen Datenverarbeitung verpflichtet (Art. 5 Abs. 2 DSGVO, Art. 24, 28 DSGVO). Darüber hinaus ergibt sich eine direkte Verpflichtung zur Erstellung des Datenschutzkonzepts für das IQTIG aus § 137a Abs. 10 SGB V i. V. m. 8. Kapitel 1. Abschnitt § 4 Abs. 4 Verfo G-BA für die Durchführung von Verfahren der sekundären Datennutzung. Der G-BA nimmt das Datenschutzkonzept ab, nachdem er es einem unabhängigen Gutachter zur Prüfung und Bewertung vorgelegt hat und dieser eine Abnahme empfiehlt.

Das IQTIG hat auf Grundlage der gesetzlichen Vorgaben der Europäischen Datenschutz-Grundverordnung, des BDSG, des SGB V sowie den Richtlinien und Verfahrensregelungen des G-BA die Ziele, Aufbau und Inhalt des Datenschutzkonzepts definiert. In Folge sind die beim IQTIG vorhandenen und künftig geplanten Datenverarbeitungsvorgänge und Maßnahmen zur Datensicherheit anhand der Zielvorgaben des Datenschutzkonzepts überprüft und bei Erforderlichkeit überarbeitet oder erweitert worden. Dieses Datenschutzkonzept soll datenschutzrechtliche Grundsätze, Prozesse und Maßnahmen abbilden, die einen datenschutzkonformen Umgang mit personenbezogenen Daten gewährleisten und Datenschutzverstöße vermeiden. Für den Fall, dass es trotz der Vorgaben im Datenschutzkonzept zu einem Datenschutzvorfall kommt, müssen die vom IQTIG getroffenen Maßnahmen und eingerichteten Prozesse so ausgestaltet sein, dass ein Schaden für die Rechte und Freiheiten der Betroffenen möglichst gering bleibt.

Die Angaben im Datenschutzkonzept basieren auf der aktuellen Gesetzeslage und entsprechen dem gegenwärtigen Stand der Technik. Sie werden im Zuge des Datenschutz-Managements regelmäßig überprüft und aktualisiert.

Das IQTIG hat ein übergeordnetes Datenschutz-Management-System (DSMS) aufgebaut. Das DSMS umfasst die Gesamtheit aller Maßnahmen, die bei der Verarbeitung personenbezogener Daten in jedem Verfahrensstadium, d. h. bei der Planung, Einführung, Durchführung und Beendigung von Verfahren, einzuhalten sind. Wesentliche Bestandteile des DSMS sind:

- Einbindung des Datenschutzbeauftragten in alle Prozesse der Verarbeitung personenbezogener Daten,
- Überprüfung der Umsetzung des Datenschutzes (z. B. Folgenabschätzung, regelmäßige interne Audits),
- Umfassende Datenschutzdokumentation (z. B. Erstellung des Verzeichnisses von Verarbeitungstätigkeiten, Dienstleister-Management nach Art. 28 DSGVO),
- Entwicklung und Pflege eines Richtlinienkonzepts für Datenschutz und Datensicherheit,
- Kontinuierliche Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für den Datenschutz,
- Konsultation der Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern keine Maßnahmen zur Eindämmung des Risikos getroffen werden,
- Abschluss von Betriebsvereinbarungen mit Bezug zum Umgang mit Mitarbeiterdaten,
- Beschwerden betroffener Personen, ggf. im Rahmen eines Eskalationsprozesses.

4 Grundsätzliche Einstellung der Einrichtung zum Datenschutz

Das IQTIG sieht sich als fachlich unabhängiges Institut in einer besonderen Funktion in der datengestützten Qualitätssicherung nach SGB V. Neben der wissenschaftlichen Entwicklung von QS-Verfahren, deren Dokumentation und Darstellung für die Weiterentwicklung, soll das IQTIG die bei den Beteiligten zu Zwecken der Qualitätssicherung in Sinne von § 299 SGB V erhobenen Daten verarbeiten.

Hieraus ergibt sich eine besondere Verpflichtung zum Schutz dieser Daten. Auch wenn das Institut im Rahmen der QS-Verfahren nur pseudonymisierte Daten erhält und daher grundsätzlich keine Möglichkeit hat, diese Daten einer bestimmten natürlichen Person zuzuordnen, handelt es sich dennoch um sensible personenbezogene Gesundheitsdaten, bei denen die Möglichkeit nicht sicher ausgeschlossen werden kann, anhand der medizinischen Daten den betreffenden Personenkreis einzugrenzen.

Daher legt das IQTIG hohen Wert auf den Schutz dieser Daten und setzt in seiner Datenschutzorganisation alle Maßnahmen um, die diesen Schutz gewährleisten. Dieser Schutz gilt in gleichem Maße für die Daten von externen Beteiligten und den Daten, die das IQTIG im Rahmen seiner internen Organisation erhebt und verarbeitet.

Die Vorgaben aus dem Datenschutzkonzept sind für die Leitung des IQTIG, die Mitarbeiterinnen und Mitarbeiter sowie befugte Dritte verbindlich. Änderungen am Datenschutzkonzept bedürfen der vorherigen Kontrolle durch den Datenschutzbeauftragten des IQTIG und ggf. der Abnahme durch den G-BA.

Die Gebote und Verbote in diesem Datenschutzkonzept gelten für jeglichen Umgang mit personenbezogenen Daten, sowohl in elektronischer Form als auch in Papierform. Ebenso beziehen sie alle Arten von Betroffenen (Beschäftigte, Patienten, Interessenten, Lieferanten, Dienstleister, etc.) in ihren Geltungsbereich ein.

5 Fachlicher und organisatorischer Hintergrund der Datenverarbeitung

Mit dem Gesetz zur Weiterentwicklung der Finanzstruktur und der Qualität in der gesetzlichen Krankenversicherung (GKV FQVG, 2014) hat der Gesetzgeber in § 137a SGB V den G-BA beauftragt, ein fachlich unabhängiges, wissenschaftliches Institut für Qualitätssicherung und Transparenz im Gesundheitswesen zu gründen. Das Institut soll sich mit der Ermittlung und Weiterentwicklung der Versorgungsqualität befassen und dem G-BA notwendige Entscheidungsgrundlagen für die von ihm gemäß § 137 zu gestaltenden Maßnahmen der Qualitätssicherung liefern.

Der G-BA hat auf der Basis dieser Vorschrift am 21. August 2014 die Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen als rechtsfähige Stiftung des privaten Rechts errichtet, die mit der ersten Sitzung des Stiftungsrats am 9. Januar 2015 ihre Arbeit aufnahm. Diese Stiftung ist Trägerin des „Instituts für Qualitätssicherung und Transparenz im Gesundheitswesen“ (IQTIG). Das IQTIG wurde durch Beschluss des Stiftungsrats gegründet. In seiner Satzung hat die Stiftung die Aufgaben des IQTIG festgelegt.

Grundlage für die Arbeit des IQTIG sind die Richtlinien und Beschlüsse des G-BA. Sie bestimmen neue Verfahren in der datengestützten Qualitätssicherung und regeln deren differenzierte Verfahrensabläufe. Hierzu hat das IQTIG eigene IT-technische Ressourcen aufgebaut, um die Aufträge des G-BA erfüllen zu können.

6 Rechtsgrundlagen der Datenverarbeitung

Das IQTIG wahrt die gesetzlichen Anforderungen an den Datenschutz. Für das IQTIG sind insbesondere folgende rechtliche Grundlagen von Bedeutung:

Das IQTIG beachtet den besonderen Schutzstandard, der an die Verarbeitung besonderer Kategorien personenbezogener Daten gestellt wird (Art. 9 DSGVO, § 22 BDSG). Demnach ist die Verarbeitung besonderer personenbezogener Daten grundsätzlich verboten, sofern die betroffene Person nicht ausdrücklich eingewilligt hat und eine Einwilligung rechtlich möglich ist (Art. 9 Abs. 2 lit. a DSGVO) oder gesetzliche Ausnahmeregelungen eingreifen (§ 22 BDSG, Art. 9 Abs. 2 DSGVO).

Für das IQTIG folgt die Erlaubnis für Verarbeitungen personenbezogener Daten zusätzlich aus den spezialgesetzlichen Anforderungen zur Qualitätssicherung (§§ 135a ff. SGB V) und zur sekundären Datennutzung gemäß § 137a Abs. 10 SGB V sowie den konkretisierenden Beschlüsse und Richtlinien des G-BA nach § 136 SGB V. Mit § 299 SGB V hat der Gesetzgeber die Voraussetzungen dafür geschaffen, dass für Zwecke der Qualitätssicherung Sozialdaten in dem erforderlichen Umfang auch ohne Einwilligung der betroffenen Patienten erhoben, verarbeitet und genutzt werden können.

Die Richtlinien und Beschlüssen sind einsehbar auf der Webseite des G-BA unter:

- <https://www.g-ba.de/informationen/beschluesse/> und
- <https://www.g-ba.de/informationen/richtlinien/>

Sollen Daten ohne gesetzliche und untergesetzliche Grundlage erhoben werden, z. B. im Zusammenhang der Entwicklung von neuen QS-Verfahren, so erfolgt dies nur nach Einwilligung der Betroffenen. Erfolgt eine Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung, sind die datenschutzrechtlichen Anforderungen an die Wirksamkeit einer Einwilligung zu wahren (Art. 6 Abs. 1 lit. a, Art. 7 DSGVO). Eine Einwilligung muss daher stets informiert, für den konkreten Fall, ausdrücklich und freiwillig erfolgen. Der Betroffene muss zudem auf die Widerrufbarkeit seiner Einwilligung sowie über die nach Art. 12 ff. DSGVO bestehenden Betroffenenrechte informiert werden.

Für den Beschäftigtendatenschutz gilt Art. 88 DSGVO i. V. m § 26 BDSG.

Für die sekundäre Datennutzung gilt § 137a Abs. 10 SGB V i. V. m. 8. Kapitel 1. Abschnitt VerFO G-BA (s. auch Nr. 7.8).

Bei jeder Datenverarbeitung sind die allgemeinen Regelungen der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) sowie des Sozialgesetzbuchs (SGB I, SGB V und SGB X) zu beachten

7 Datenschutzbezogene Anforderungen bezogen auf die Verarbeitungsvorgänge / Verarbeitungstätigkeiten beim IQTIG

Die Verarbeitungsvorgänge im IQTIG lassen sich in vier Gruppen einteilen:

- a. QS-Verfahren:
Daten, die für die Entwicklung und Durchführung von QS-Verfahren verarbeitet werden.
- b. Teilnehmerverwaltung:
Daten, die von Beteiligten an Fachgruppen und Expertengremien im IQTIG sowie weiteren externen Beteiligten stammen, die im Rahmen der Aufgaben des IQTIG mit diesem zusammenarbeiten.
- c. Interne Daten:
Daten von Mitarbeiterinnen und Mitarbeitern des IQTIG, Bewerberinnen und Bewerbern sowie externen Partnern für die interne Verwaltung.
- d. Sekundäre Datennutzung:
Daten aus den QS-Verfahren und Daten von Antragstellern.

7.1 Grundsätze der Verarbeitung

Die Verarbeitung von personenbezogenen Daten muss den Grundsätzen des Art. 5 DSGVO folgen. In diesem Kapitel werden die Grundsätze nach Art. 5 Abs. 1. lit. b - f DSGVO beschrieben.

7.1.1 Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- a. QS-Verfahren:

Das IQTIG darf die im Rahmen der QS-Verfahren erhaltenen Daten nur zu den Zwecken der Qualitätssicherung verarbeiten (§ 137a Abs. 3 SGB V in Verbindung mit § 299 SGB V). Die Zwecke ergeben sich aus den Richtlinien und Beschlüssen des G-BA.

b. Teilnehmerverwaltung:

Daten von externen Beteiligten (z. B. Experten, Gremienmitglieder) werden mit deren Einwilligung nur zum Zweck der Kontaktaufnahme und der Übermittlung von relevanten Informationen verarbeitet.

c. Interne Daten:

Daten der Mitarbeiterinnen und Mitarbeiter des IQTIG werden zu Zwecken des Beschäftigungsverhältnisses (§ 26 BSDG) oder aufgrund von Einwilligungen (Art. 6 Abs. 1 lit. a, Art 7 DSGVO) verarbeitet.

d. Sekundäre Datennutzung:

Im Rahmen der sekundären Datennutzung können die erhobenen Daten auf Antrag auch „für Zwecke der wissenschaftlichen Forschung“ und „zur Weiterentwicklung der Qualitätssicherung“ und damit außerhalb des ursprünglichen Zweckzusammenhangs genutzt werden (§ 137a Abs. 10 SGB V). Der neue Zweck ergibt sich aus dem Antrag für die sekundäre Datennutzung und wird durch die Entscheidung über den Antrag vom G-BA festgelegt.

7.1.2 Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

a. QS-Verfahren:

Das IQTIG hat zu Zwecken der Qualitätssicherung nur die Daten zu erheben, die für die Messung und Darstellung der Qualität tatsächlich erforderlich sind. Die zu erhebenden Daten sind für die bestehenden Verfahren in den jeweiligen Richtlinien abschließend aufgezählt. Eine nachträgliche Ergänzung der Daten ist nur im Ausnahmefall und nach nachvollziehbarer Begründung und datenschutzrechtlicher Prüfung erlaubt. Der Umfang der zu erhebenden Daten wird vom G-BA in seinen Richtlinien und Beschlüssen festgelegt.

Das IQTIG erhebt Qualitätssicherungsdaten nach dem Grundsatz der pseudonymisierten Stichprobenerhebung. Eine Vollerhebung ist nur im Ausnahmefall erlaubt (§ 299 Abs. 1 S. 5 SGB V), beispielsweise wenn eine Stichprobenerhebung nicht ausreichend wäre, um die Versorgungsqualität einer Einrichtung zuverlässig erfassen zu können. Die Erforderlichkeit einer Vollerhebung begründet der G-BA jeweils in seinen Richtlinien.

Bei der Entwicklung neuer Verfahren sind die für das künftige Verfahren zu erhebenden Daten auf das erforderliche Maß zu reduzieren. Die Daten sind erforderlich, wenn sie für die Erreichung des Verfahrenszwecks unverzichtbar und aufgrund wissenschaftlicher Kriterien für die Qualitätssicherung geeignet sind. Die Erforderlichkeit eines Datums ist nachvollziehbar zu begründen.

b. Teilnehmerverwaltung

Für die Beteiligten in den Fachgremien und Expertengruppen des IQTIG werden die Kontaktdaten zur Übermittlung von notwendigen Informationen erhoben. Hierzu erfolgt auch eine Regist-

rierung für ein Web-basiertes Dokumentenaustauschportal (DokEx), durch das Beratungsunterlagen, Ergebnisse und Berichte zur Verfügung gestellt werden. Die Registrierung dient auch zur Bereitstellung von Auswertungen im Rahmen der QS-Verfahren unter den Bedingungen der Richtlinien des G-BA. Es werden nur die hierzu notwendigen Informationen abgefragt.

c. Interne Daten:

Es werden nur Daten erhoben, die für die Zwecke des Beschäftigungsverhältnisses oder im Rahmen der geschäftlichen Beziehungen mit externen Vertragspartnern notwendig sind.

d. Sekundäre Datennutzung:

Es werden keine zusätzlichen QS-Daten erhoben, da die Daten für die sekundäre Datennutzung aus den bereits erhobenen Daten aus den QS-Verfahren stammen. Daten der Antragsteller werden nur nach den Vorgaben aus der Verfahrensordnung des G-BA erhoben (Anlagen I und II zum 8. Kapitel 1. Abschnitt VerFO G-BA).

7.1.3 Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

a. QS-Verfahren:

Das IQTIG erhebt in der Regel personenbezogene Daten nicht unmittelbar von den Betroffenen, sondern erhält diese entweder von den Leistungserbringern (direkte Verfahren) oder von den Datenannahmestellen auf Landesebene (indirekte Verfahren). Zudem erhält das IQTIG personenbezogene Daten nur in pseudonymisierter Form. Die Richtigkeit der Daten ist damit im Zeitpunkt der Datenverarbeitung durch das IQTIG bereits vorausgesetzt.

Grundlage für die Richtigkeit der Daten ist somit das Verfahren zur Datenübermittlung zwischen den Beteiligten. Vorgaben zur Datenübermittlung trifft der G-BA in den jeweils einschlägigen Beschlüssen und Richtlinien.

Sofern das IQTIG offensichtliche Abweichungen bei der Datenübermittlung feststellt, dokumentiert es diesen Vorfall und weist die Beteiligten darauf hin. Es besteht jedoch darüber hinaus keine Verpflichtung des IQTIG, Datenübermittlungen regelmäßig auf ihre Richtlinienkonformität zu überprüfen.

b. Teilnehmerverwaltung, interne Daten:

Soweit in der Teilnehmerverwaltung oder bei den internen Daten des IQTIG Unrichtigkeiten festgestellt werden, werden diese Daten unverzüglich korrigiert oder gelöscht. Hierzu können sich die Betroffenen direkt an das IQTIG wenden (**Anlage 6**).

c. Sekundäre Datennutzung:

Hinsichtlich der QS-Daten wird auf Nr. 7.1.3 lit. a. verwiesen. Hinsichtlich der Daten der Antragsteller wird wie unter Nr. 7.1.3 lit. b. verfahren.

7.1.4 Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Das IQTIG hat zur Einhaltung und Dokumentation der Speicherfristen ein Löschkonzept (**Anlage 7**) erstellt. Unter Beachtung der gesetzlichen Aufbewahrungsfristen werden personenbezogene Daten nach Zweckfortfall gelöscht.

Nach Abschluss eines Qualitätssicherungsverfahrens werden die zugehörigen Daten anonymisiert, sofern vom G-BA keine andere Regelung getroffen wurde.

a. QS-Verfahren:

Nach Ablauf eines Auswertungszeitraums werden die von der Vertrauensstelle erstellten und den QS-Daten hinzugefügten Patientenpseudonyme gelöscht. Damit werden die primären personenidentifizierenden Daten entfernt und die QS-Daten weitestgehend anonymisiert. Da jedoch nicht auszuschließen ist, dass in einzelnen Fällen anhand der verbleibenden medizinischen Daten der betreffende Personenkreis eingrenzbar ist, unterliegen auch diese Daten im IQTIG dem besonderen Schutz.

b. Teilnehmerverwaltung:

Personenbezogene Daten in der Teilnehmerverwaltung werden nach Beendigung der für die Teilnehmerverwaltung relevanten Funktion oder bei Widerruf der Einwilligung zur Speicherung gelöscht.

c. Interne Daten:

Personaldaten werden für die Dauer der Beschäftigung beim IQTIG und darüber hinaus auf der Grundlage gesetzlicher Verpflichtungen aufbewahrt (z. B. sozialrechtliche Aufbewahrungspflichten).

Daten von Bewerberinnen und Bewerbern werden im Falle der Übernahme in ein Beschäftigungsverhältnis in die Personalakte übernommen. Andernfalls werden die Daten sechs Monate nach Absage gelöscht, es sei denn, es liegt eine Einwilligung zur weiteren Speicherung vor.

Daten von externen Dienstleistern werden im Rahmen der Geschäftsbeziehung und der vertraglichen Bedingungen sowie haushalts- und ggf. steuerrechtlichen Vorgaben aufbewahrt.

d. Sekundäre Datennutzung:

Für die sekundäre Datennutzung werden bereits anonymisierte Daten verwendet (s. unter a.). Daher liegen hier keine personenbezogenen oder personenbeziehbaren Daten mehr vor, die gelöscht werden müssen.

7.1.5 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter

oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

a. Für alle Verarbeitungsvorgänge

Die für das IQTIG geltenden technischen und organisatorischen Maßnahmen sind gesondert unter **Anlage 1** „Technische und organisatorische Maßnahmen“ und **Anlage 2** „IT Datenschutzmaßnahmen“ aufgeführt.

Es sind verbindliche schriftliche Arbeitsanweisungen veröffentlicht. Erläutert wird dort bspw. der Umgang mit vertraulichen Unterlagen, unbekanntem Anhängen von E-Mails sowie Passwörtern (**Anlagen 3 und 4**).

b. Sekundäre Datennutzung:

Zusätzlich ist für Durchführung der sekundären Datennutzung die Anonymisierung der Auswertungsergebnisse und eine gesonderte datenschutzrechtliche Prüfung des Antrags vorgegeben (siehe auch Nr. 7.8).

7.2 Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1. lit. a DSGVO).

Die Verarbeitung der Daten im IQTIG erfolgt gem. Art 6 und Art. 9 DSGVO entweder aufgrund ausdrücklicher Einwilligung der oder des Betroffenen oder auf gesetzlicher Grundlage (SGB V, Richtlinien des G-BA). Um Sorgfalt und Transparenz bei Datenverarbeitungen zu gewährleisten, informiert das IQTIG in leichter und verständlicher Sprache bei der Erhebung der Daten von Betroffenen (Direkterhebung) und bei Übermittlungen von Daten (Dritterhebung) über Art, Zweck, Umfang, Rechte und Risiken der Datenverarbeitung nach Art. 13 und Art. 14 DSGVO.

Betroffene sollen dadurch die mit der Datenverarbeitung verbundenen Risiken abschätzen und die Rechte wahrnehmen können, die ihnen nach der Datenschutz-Grundverordnung zustehen.

a. QS-Verfahren:

Die Verarbeitung der QS-Daten erfolgt auf der Grundlage der Richtlinien des G-BA gem. § 136 SGB V unter Beachtung der Vorgaben zum Datenschutz gem. § 299 SGB V.

b. Teilnehmerverwaltung:

Die Teilnehmer willigen bei der Registrierung der Erhebung und Verarbeitung ihrer Daten i. S. v. Art. 7 DSGVO ein.

c. Interne Daten:

Personaldaten werden zum Zwecke des Beschäftigungsverhältnisses gem. § 26 BSDG erhoben. Weitergehende Daten werden nur erhoben, wenn hierzu eine Betriebsvereinbarung oder eine Einwilligung vorliegt.

d. Sekundäre Datennutzung:

Die Verarbeitung der QS-Daten zu Zwecken der sekundären Datennutzung erfolgt auf Grundlage des § 137a Abs. 10 SGB V i. V. m. dem 8. Kapitel 1. Abschnitt VerFO G-BA.

7.3 Datenschutz durch Technikgestaltung

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

Die für das IQTIG geltenden technischen und organisatorischen Maßnahmen sind gesondert unter **Anlage 1** und **2** aufgeführt und gelten für alle Verarbeitungsvorgänge.

7.4 Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Institutsleitung führt zu diesem Zweck ein Managementsystem für Informationssicherheit (ISMS) ein (Softwaretool: „verinice“ der Fa. SerNet).

Die technischen und organisatorischen Maßnahmen sind fortlaufend zu dokumentieren.

7.5 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Betroffene

Bei der Verletzung des Schutzes personenbezogener Daten, etwa durch Abfluss von personenbezogener Daten nach einem IT-Vorfall oder durch unbefugten Zugriff auf Daten nach dem Verlust eines Notebooks, ist innerhalb von 72 Stunden eine Meldung an die Aufsichtsbehörde für

den Datenschutz abzusetzen. Soweit die Voraussetzungen des Art. 34 DSGVO erfüllt sind, müssen auch die von der Verletzung Betroffenen benachrichtigt werden.

Vor der Meldung an die Aufsichtsbehörde und der Benachrichtigung der Betroffenen ist der DSB anzuhören. Der Inhalt von Meldung und Benachrichtigung ist mit ihm abzustimmen.

Die Abteilung des IQTIG, in deren Verantwortungsbereich der Datenschutzvorfall fällt, schlägt unverzüglich Maßnahmen zur Behebung der Verletzung und zur Abmilderung möglicher nachteiliger Auswirkungen vor. Soweit Maßnahmen keinen Aufschub dulden, sind sie umgehend zu ergreifen. Sämtliche Maßnahmen werden dokumentiert.

Wenn von einer Meldung abgesehen werden kann, sind die Gründe dafür gem. Art. 33 Abs. 5 DSGVO zu dokumentieren.

7.6 Datenschutz-Folgenabschätzung

Um die Rechtmäßigkeit der Datenverarbeitung und insbesondere die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen zu können, sind alle datenschutzrelevanten Dokumente so vorzuhalten, dass sie in ihrer Gesamtheit ohne Verzögerung abgerufen werden können.

Über alle Verarbeitungstätigkeiten, die der Zuständigkeit des IQTIG unterliegen, wird ein Verzeichnis geführt (**Anlage 5**). Dieses Verzeichnis enthält sämtliche Angaben, die nach Art. 30 DSGVO erforderlich sind.

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, wird vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt. Die Datenschutz-Folgenabschätzung wird nach Maßgabe des Art. 35 DSGVO erstellt.

Der Datenschutzbeauftragte erstellt einen jährlichen Tätigkeitsbericht für die Institutsleitung und den G-BA. Darin werden insbesondere die Wirksamkeit und der Grad der Umsetzung dieses Datenschutzkonzepts beurteilt.

Alle Maßnahmen werden durch das im IQTIG verwendete Managementsystem für Informationssicherheit (Information Security Management System - ISMS) verwaltet und unterstützt.

7.7 Beachtung der Betroffenenrechte

Von der Verarbeitung personenbezogener Daten im Rahmen der gesetzlichen Qualitätssicherung beim IQTIG sowie bei den übrigen Verarbeitungsvorgängen sind folgende Personengruppen betroffen:

- Patientinnen und Patienten
- Mitarbeiterinnen und Mitarbeiter der Krankenhäuser und sonstiger Leistungserbringer, Ärztinnen/Ärzte
- Mitarbeiterinnen und Mitarbeiter der Versendestelle bei Patientenbefragungen

- Mitarbeiterinnen und Mitarbeiter der Vertrauensstelle
- Mitarbeiterinnen und Mitarbeiter des IQTIG
- Mitarbeiterinnen und Mitarbeiter des G-BA und seiner Träger
- Mitarbeiterinnen und Mitarbeiter der die Daten annehmenden Stellen
- Personen in den benannten Stellen auf Landesebene
- Personen in den Lenkungsorganen auf Bundes- und Landesebene
- Personen in den Fachgremien und Expertengruppen auf Bundes- und Landesebene
- Personen bei Softwareanbietern
- Personen bei Lieferanten, Beratern und Auftragnehmer
- Personen bei Berichterstellern im Rahmen der QS-Dialyse

Soweit es sich bei den Betroffenen um Patientinnen und Patienten handelt, deren Daten aufgrund gesetzlicher oder untergesetzlicher Vorschriften im Rahmen von QS-Verfahren erhoben und verarbeitet werden, kann das IQTIG nur in allgemeiner Form (z. B. auf seiner Homepage) informieren. Denn die Daten, die das Institut verarbeitet, werden ihm pseudonymisiert zur Verfügung gestellt, so dass eine Identifikation durch das IQTIG nicht möglich ist.

7.7.1 Transparenz und Modalitäten der Betroffenenrechtsausübung

Betroffene Personen, insbesondere Beschäftigte, Patienten sowie Ansprechpartner bei Dienstleistern und Lieferanten, haben das Recht auf Transparenz der Verarbeitung (insbesondere Informationspflichten nach Art. 13, 14 DSGVO sowie Auskunftsrecht nach Art. 15 DSGVO), auf Richtigkeit der Verarbeitung (insbesondere Recht auf Berichtigung nach Art. 16 DSGVO, auf Löschung nach Art. 17 DSGVO und auf Einschränkung der Verarbeitung nach Art. 18 DSGVO) sowie auf Beschränkung der Verarbeitung (insbesondere Widerspruchsrecht nach Art. 21 DSGVO).

Die betroffenen Personen werden bei der Ausübung ihrer Rechte durch das IQTIG unterstützt und sind in einer Richtlinie festgelegt (**Anlage 6**).

Bei der Bearbeitung von Anträgen ist die Identität der betroffenen Person zweifelsfrei festzustellen. Die Erteilung von Auskünften ist zu dokumentieren.

7.7.2 Informationspflicht und Auskunft zu personenbezogenen Daten des Betroffenen

Die Institutsleitung trifft geeignete Maßnahmen, um betroffenen Personen alle Informationen gemäß den Art. 13 und 14 DSGVO und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34 DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache innerhalb der gesetzlichen Fristen zu übermitteln.

Sollten Dritte, insbesondere Behörden, Informationen über betroffene Personen fordern, beispielsweise über Beschäftigte des IQTIG oder Patienten, ist eine Weitergabe von Informationen nur zulässig, wenn

- eine gesetzliche Norm zur Auskunft verpflichtet oder
- das IQTIG ein berechtigtes Interesse an der Weitergabe der Informationen hat und
- die Identität des anfragenden Dritten zweifelsfrei feststeht.

7.7.3 Berichtigung und Löschung, Datenübertragbarkeit

Die Institutsleitung trifft geeignete Maßnahmen, um einem Verlangen von betroffenen Personen auf Berichtigung, Löschung oder Datenübertragung nach den Art. 16 bis 20 DSGVO nachzukommen.

Soweit es sich bei den Betroffenen um Patientinnen und Patienten handelt, deren Daten aufgrund gesetzlicher oder untergesetzlicher Vorschriften im Rahmen von QS-Verfahren erhoben und verarbeitet werden, kann das IQTIG jedoch eine Zuordnung von Daten zu Personen nicht vornehmen. Denn die Daten, die das Institut verarbeitet, werden ihm pseudonymisiert zur Verfügung gestellt, so dass eine Identifikation durch das IQTIG nicht möglich ist.

7.7.4 Widerspruchsrecht

Die Institutsleitung trifft geeignete Maßnahmen, um eine weitere Verarbeitung zu unterbinden, wenn eine betroffene Person ihr Recht auf Widerspruch (Art. 21 DSGVO) ausübt.

7.8 Datenverarbeitung beim Verfahren der sekundären Datennutzung

Mit dem am 1. Januar 2015 in Kraft getretenen Gesetz zur Weiterentwicklung der Finanzstruktur und der Qualität in der gesetzlichen Krankenversicherung (GKV-Finanzstruktur- und Qualitäts-Weiterentwicklungsgesetz – GKV-FQWG) hat der Gesetzgeber in § 137a Absatz 10 SGB V die Voraussetzungen zur Nutzung der Daten aus der einrichtungsübergreifenden Qualitätssicherung für Zwecke der Forschung und Weiterentwicklung der Qualitätssicherung (sog. sekundäre Datennutzung) geregelt. Der G-BA hat in seiner Verfahrensordnung (VerfO G-BA) die Einzelheiten hierzu festgelegt.

Ergänzend zum Datenschutzkonzept werden im Folgenden die zusätzlichen speziellen Bedingungen für die sekundäre Datennutzung beschrieben.

7.8.1 Besondere Regelungen zur sekundären Datennutzung

Gemäß 8. Kapitel 1. Abschnitt § 4 Abs. 4 VerfO G-BA werden zusätzliche Anforderungen an den Datenschutz bei der Durchführung der sekundären Datennutzung nach § 137a Abs. 10 SGB V gestellt. Die folgenden Bestimmungen ergänzen die vorangegangenen bei der Durchführung der sekundären Datennutzung durch das IQTIG.

Die Durchführung der sekundären Datennutzung ist nur zulässig, wenn die im 8. Kapitel 1. Abschnitt VerfO G-BA geregelten Voraussetzungen erfüllt sind und dem Antrag auf sekundäre Datennutzung durch den G-BA stattgegeben wurde.

Im Einzelnen getroffene Maßnahmen:

- Das IQTIG nimmt eine datenschutzrechtliche Vorprüfung nach § 7 Abs. 1 Nr. 5 8. Kapitel 1. Abschnitt VerfO G-BA vor.
- Das IQTIG stellt sicher, dass die Auswertung nur in geschützter Umgebung in den eigenen Räumlichkeiten stattfindet und die Daten ausschließlich durch Mitarbeiterinnen oder Mitarbeiter des IQTIG bearbeitet werden.
- Die Antragstellerin oder der Antragsteller erhält keinen Zugriff auf die erhobenen Daten.

- Die Auswertungsergebnisse werden der Antragstellerin oder dem Antragsteller nur anonymisiert und in aggregierter Form zur Verfügung gestellt. Die Anonymisierung erfolgt so, dass eine Identifizierung einzelner Personen oder Leistungserbringer auch unter Nutzung von Zusatzwissen der Antragstellerin oder des Antragstellers sicher ausgeschlossen ist.
- Das Zusammenführen mit anderen Daten als denen, die im Rahmen der verpflichtenden Maßnahmen zur Qualitätssicherung nach § 136 Absatz 1 Satz 1 SGB V erhoben wurden, zum Zwecke einer Auswertung ist möglich, soweit diese Daten ausschließlich anonym sind und sichergestellt werden kann, dass eine Identifizierung einzelner Personen oder Leistungserbringer auch nach der Zusammenführung ausgeschlossen ist.

7.8.2 Anträge zur sekundären Datennutzung durch das IQTIG

Das IQTIG selber kann ebenfalls Anträge zur sekundären Datennutzung stellen. Hierbei werden die in diesem Datenschutzkonzept vorgesehenen Regelungen gleichermaßen eingehalten.

Mitarbeiterinnen und Mitarbeiter des IQTIG, die den Antrag auf sekundäre Datennutzung für das IQTIG erarbeitet haben, werden nicht an dessen Bearbeitung beteiligt und erhalten insoweit keinen Zugriff auf die auszuwertenden Daten.

7.8.3 Anträge auf sekundäre Datennutzung durch Mitarbeiterinnen oder Mitarbeiter

Mitarbeiterinnen und Mitarbeiter des IQTIG, die für sich selber als natürliche Person einen Antrag auf sekundäre Datennutzung gestellt haben, werden weder an der Vorprüfung und Einschätzung des Antrags, noch an dessen Bearbeitung beteiligt.

7.8.4 Anonymisierung der Qualitätssicherungsdaten für die sekundäre Datennutzung

Das IQTIG ist verpflichtet, Auswertungsergebnisse aus dem Verfahren der sekundären Datennutzung nur in anonymisierter Form an den Antragssteller zu übermitteln.

Die Anonymisierung der Auswertungen erfolgt auf Grundlage eines eigenen Konzepts nach dem aktuellen Stand der Technik (BSI-Standards)¹. Das Anonymisierungsverfahren muss sicherstellen, dass eine Reidentifizierung natürlicher Personen oder Leistungserbringer auch unter Zusatzwissen des Antragstellers sicher ausgeschlossen ist. Die Anonymisierung von Qualitätssicherungsdaten wird durch den Datenschutzbeauftragten des IQTIG auf ihre Datenschutzkonformität geprüft.

Der Antrag auf sekundäre Datennutzung ist abzulehnen, wenn eine Reidentifizierung nicht sicher ausgeschlossen werden kann.

Die zuständigen Mitarbeiterinnen oder Mitarbeiter des IQTIG werden auf die Einhaltung der ergänzenden Bestimmungen zur sekundären Datennutzung im Datenschutzkonzept geschult. Hat eine Mitarbeiterin oder ein Mitarbeiter bei Bearbeitung eines Antrags Zweifel in Bezug auf die

¹ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
(Vgl. auch Tragende Gründe zum Beschluss des G-BA vom 20.04.2017:
https://www.g-ba.de/downloads/40-268-4335/2017-04-20_VerFO_Ergaenzung-8es-Kapitel_TrG.pdf
und Drucksache des Deutschen Bundestages Drs 18/1307, S. 37.)

Anonymität der Daten, ist der Datenschutzbeauftragte des IQTIG vor Freigabe der Auswertungsergebnisse hinzuzuziehen.

8 Akteure und Beteiligte an der Verarbeitung

8.1 Verantwortlicher / Verantwortliche der Datenverarbeitung

Das IQTIG ist „Verantwortlicher“ im Sinne des SGB X und der DSGVO (Art. 4 Nr. 7 DSGVO, § 67 Abs. 9 SGB X). Seine Tätigkeit richtet sich nach § 137a SGB V und den Beschlüssen und Richtlinien des G-BA.

8.1.1 Verantwortlichkeit der Institutsleitung

Die Leitung des IQTIG trägt die persönliche Verantwortung für die Durchsetzung der für Datenschutz und Datensicherheit erforderlichen Maßnahmen. Die Anforderungen an Datenschutz und Datensicherheit werden bei Entscheidungen der Institutsleitung im erforderlichen Maße berücksichtigt.

8.1.2 Datenschutzbeauftragter

Das IQTIG hat nach Maßgabe der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) einen Datenschutzbeauftragten (DSB) benannt:

Herrn Martin Schüller
Leiter Stabsbereich Recht
Tel.: 030 / 585826-130
E-Mail: datenschutz@iqtig.org

Der DSB unterrichtet und berät die Institutsleitung und die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO und anderen datenschutzrechtlichen Vorschriften.

Der DSB überwacht die Einhaltung der DSGVO, anderer datenschutzrechtlicher Vorschriften sowie dieses Datenschutzkonzepts und sensibilisiert die Beschäftigten für den Schutz personenbezogener Daten.

Betroffene Personen können den DSB zu allen Fragen zu Rate ziehen, die mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehen. Sämtliche Anfragen werden vertraulich behandelt.

Die Institutsleitung stellt sicher, dass der DSB bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Sie unterstützt den DSB bei der Erfüllung seiner Aufgaben, indem sie die erforderlichen Ressourcen zur Verfügung stellt und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen ermöglicht.

Der DSB ist für die Kommunikation mit der Aufsichtsbehörde für den Datenschutz zuständig.

8.1.3 Mitarbeiterinnen- und Mitarbeitersensibilisierung

Jeder Mitarbeiterin und jedem Mitarbeiter ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Sie sind daher vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit schriftlich zu verpflichten.

Beschäftigte des IQTIG werden außerdem auf das Sozialgeheimnis nach § 35 Abs. 1 S. 1 SGB I verpflichtet. Mit der Information zur Vertraulichkeit und zum Sozialgeheimnis wird für eine erste Unterweisung ein Merkblatt ausgegeben, das den Mitarbeiterinnen und Mitarbeitern die Zusammenhänge und Handlungsverpflichtungen transparent macht.

Der Umgang mit den informationstechnischen Einrichtungen durch die Mitarbeiterinnen und Mitarbeiter ist in einer IT-Nutzungs-Richtlinie geregelt (**Anlage 4**). Der Umgang mit Passwörtern ist in einer Passwort-Richtlinie geregelt (**Anlage 3**).

In Abstimmung mit dem Datenschutzbeauftragten finden darüber hinaus Präsenz- oder webbasierte Schulungen statt, um den datenschutzgerechten Umgang in der täglichen Arbeitspraxis zu gewährleisten. Die Teilnahme an den Schulungen wird dokumentiert und protokolliert. Alle Teilnehmer erhalten hierüber eine Teilnahmebescheinigung.

Häufigkeit und Inhalt der Schulungen orientieren sich nach dem Bedarf der einzelnen Abteilungen. Während eine Grundlagenschulung zum Datenschutz und zur Datensicherheit für alle Beschäftigten mit Bezug zu personenbezogenen Daten verpflichtend ist, werden Aufbauschulungen für die Bereiche Personal, Buchhaltung, IT, Verfahrensentwicklung, Verfahrensgrundlagen, Verfahrensmanagement, Patientenbelange, Evaluation, Sozialdaten und Biometrie u. a. angeboten

8.1.4 Datenübermittlung

Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn das Drittland, in dem der Empfänger seinen Sitz hat, kein angemessenes Datenschutzniveau bietet oder andere geeignete Garantien nicht vorhanden sind. Eine solche Garantie besteht insbesondere in Standarddatenschutzklauseln, die mit dem Empfänger abgeschlossen werden.

Das IQTIG verarbeitet personenbezogene Daten ausschließlich in Deutschland.

8.2 Auftragsverarbeiter

Dienstleister und Lieferanten mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Erfolgt eine Verarbeitung im Auftrag des IQTIG, muss der Auftragsverarbeiter durch geeignete technische und organisatorische Maßnahmen hinreichend Garantien dafür bieten, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO und dem SGB X erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Die Auswahl von Dienstleistern sowie Lieferanten ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang,

- Technisch-organisatorische Sicherheitsmaßnahmen,
- Erfahrung des Anbieters im Markt,
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.).

Vor der Beauftragung ist der DSB zu informieren, sodass er überprüfen kann, ob der erforderliche Vertrag nach Art. 28 DSGVO abgeschlossen worden ist.

Die Vereinbarungen mit Dienstleistern und Lieferanten werden in einem Dokumentenmanagementsystem (Projektron BCS) erfasst, damit der Abschluss von Verträgen nach Art. 28 DSGVO nachvollziehbar und der Inhalt der Verträge einsehbar ist.

Auftragsverarbeiter sind im Hinblick auf die vertraglich vereinbarten technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

Soweit Erfüllungsgehilfen potentiellen Zugriff auf die entsprechenden Daten beim IQTIG erhalten, werden die datenschutz- und vertragsrechtlich erforderlichen Vertraulichkeitserklärungen eingeholt.

9 Aufbewahrungsfristen im Kontext der Zweckbestimmung

a. QS-Verfahren / Sekundäre Datennutzung:

Im Rahmen der QS-Verfahren ergeben sich die Aufbewahrungsfristen aus den Bestimmungen der jeweiligen Richtlinien und Beschlüssen des G-BA. Darüber hinaus werden die Daten zu Zwecken der sekundären Datennutzung nach § 137a Abs. 10 SGB V gespeichert. Daten bei Entwicklung werden nach Fertigstellung anonymisiert (s. auch Einwilligung)

b. Teilnehmerverwaltung:

Personenbezogene Daten werden nur solange aufbewahrt, wie die betroffene Person Zugriff auf entsprechende Informationen im Dokumentenaustauschportal des IQTIG benötigt, z. B. als Mitglied einer Fachgruppe oder eines Expertengremiums, und eine wirksame Einwilligung zur Speicherung vorliegt.

c. Interne Daten:

Personaldaten werden nach den gesetzlichen Vorgaben gespeichert. Die Aufbewahrungsfristen richten sich nach den einschlägigen sozial- und steuerrechtlichen Bestimmungen (im Allgemeinen 10 Jahre).

Daten von Bewerberinnen und Bewerbern werden spätestens sechs Monate nach der Ablehnung der Bewerbung gelöscht, es sei denn, die Person hat in eine längere Speicherung eingewilligt (z. B. um in einen Bewerberpool für spätere freie Stellen aufgenommen zu werden). Bei Einstellung der Bewerberin bzw. des Bewerbers werden die Daten in die Personalakte übernommen.

10 Konkrete Umsetzung der Anforderungen (Kapitel 7 bis 9) bezogen auf die relevanten Verarbeitungstätigkeiten des IQTIG

Die konkrete Umsetzung der oben beschriebenen Anforderungen ergibt sich aus dem Verzeichnis von Verfahrenstätigkeiten gem. Art. 30 DSGVO (**Anlage 5**). Bezogen auf die vier Gruppen von Verarbeitungsvorgängen (QS-Verfahren/Teilnehmerverwaltung/interne Daten/sekundäre Datennutzung - s. Nr. 7) werden die folgenden Verfahren beschrieben:

- a. QS-Verfahren:
 - Indirekte Verfahren nach QSKH-RL
 - Follow-up Verfahren nach QSKH-RL
 - Direkte Verfahren nach QSKH-RL
 - Datenübermittlung zum Qualitätsbericht
 - Bericht zum strukturierten Dialog
 - Datenvalidierung nach QSKH-RL und planQI-RL
 - Verfahren nach planQI-RL
 - Verfahren nach DeQS-RL
 - Verfahren nach QSD-RL
 - Risikostatistik nach QSKH-RL
 - Sollstatistik nach QSKH-RL und DeQS-RL
 - Strukturierter Dialog bzw. Stellungnahmeverfahren
 - Nicu-Verfahren
- b. Teilnehmerverwaltung:
 - DokEx - Dokumentenaustauschportal
- c. Interne Daten:
 - Personaldatenverwaltung
 - Lohn- und Gehaltsabrechnung
 - Bewerbungsmanagement
 - Reisekostenabrechnung
 - Zeiterfassung Mitarbeiter*innen
 - Bibliotheksverwaltung
- d. Sekundäre Datennutzung

11 Definitionen, Begriffsbestimmungen und Abkürzungen

Nachfolgend sind Begrifflichkeiten definiert, die für den Datenschutz beim IQTIG wesentlich sind. Die Definitionen dienen dem besseren Verständnis und der Lesbarkeit des Datenschutzkonzepts. Sie sind nicht abschließend zu verstehen.

- **Qualitätssicherung:**

Der Begriff der Qualitätssicherung umfasst alle Maßnahmen i. S. d. §§ 136 ff. SGB V, die der Messung und Darstellung der Qualität im Gesundheitswesen dienen.

- **Sekundäre Datennutzung:**

Sekundäre Datennutzung ist die Nutzung des durch die Qualitätssicherung erlangten Datenbestands zu Zwecken der medizinischen Forschung und zur Weiterentwicklung der Qualitätssicherung (§ 137a Abs. 10 SGB V).

- **Personenbezogene Daten:**

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO).

- **Sozialdaten:**

Sozialdaten sind personenbezogene Daten, die ein Sozialleistungsträger in Erfüllung einer Aufgabe nach dem Sozialgesetzbuch erhebt, verarbeitet oder nutzt (§ 69 SGB X).

- **Gesundheitsdaten:**

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO).

- **Genetische Daten**

Genetische Daten sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden (Art. 4 Nr. 13 DSGVO)

- Qualitätssicherungsdaten:

Qualitätssicherungsdaten sind Behandlungsdaten, die Angaben zum Gesundheitszustand der Betroffenen oder über die erbrachten diagnostischen und therapeutischen Leistungen enthalten sowie weitere, in den themenspezifischen Bestimmungen festzulegende relevante Daten. Qualitätssicherungsdaten können z. B. sein: Angaben zum Geburtsjahr, Geschlecht, Postleitzahl und Bundesland des Patientenwohnorts, Behandlungsverlauf, behandelndes Krankenhaus). Bei Qualitätssicherungsdaten handelt es sich daher hauptsächlich um Gesundheitsdaten im Sinne des Art. 4 Nr. 17 DSGVO.

- Administrative Daten:

Administrative Daten umfassen Daten, die zur Prüfung auf Vollständigkeit, Vollzähligkeit und Plausibilität geeignet sind, sowie weitere, meldebezogene Daten (z. B. Standort, Zeitstempel und Nummer des Datensatzes, das Thema der jeweiligen Datenlieferung). Administrative Daten haben überwiegend keinen Personenbezug. Administrative Daten mit Personenbezug können hingegen sein: Angaben über Kommunikationspartner.

Die im jeweiligen Qualitätssicherungsverfahren oder im Rahmen der Patientenbefragung zu erhebenden Daten sind den Richtlinien oder Beschlüssen des G-BA zu entnehmen. Die Richtlinien und Beschlüsse stehen auf der Webseite des G-BA zum Download zur Verfügung.

- (Daten-)Verarbeitung:

Eine Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO).

- Pseudonymisierung:

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Nr. 5 DSGVO). Anders als bei der Anonymisierung kann bei der Pseudonymisierung der Personenbezug über zuvor festgelegte Zuordnungsregelungen wieder hergestellt werden. Die Zuordnungsregelungen sind dabei nur der Zuordnungsstelle (Vertrauensstelle) bekannt.

- Anonymisierung:

Anonymisierung bedeutet, 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 bestimmaren natürlichen Person zugeordnet werden können (§ 67 Abs. 8 SGB X).

12 Anlagen

Anlage 1: Technische und organisatorische Maßnahmen

Anlage 2: IT Datenschutzmaßnahmen

Anlage 3: Passwort-Richtlinie

Anlage 4: IT Nutzungs-Richtlinie

Anlage 5: Verzeichnis von Verfahrenstätigkeiten

Anlage 6: Richtlinie Betroffenenrechte

Anlage 7: Löschkonzept

Anlage 1:

Technische und organisatorische Maßnahmen

Wesentlicher Bestandteil des Datenschutzes ist die Gewährleistung von Datensicherheit durch die Einrichtung erforderlicher technischer und organisatorischer Maßnahmen (Art. 32 DSGVO und § 78a SGB X). Personenbezogene Daten und die diese Daten verarbeitenden Datenverarbeitungsanlagen, d. h. die Hard- und Software, sind vor unbefugter Kenntnisnahme Dritter, vor Manipulation und vor Verlust zu schützen. Das IQTIG verwendet sein ISMS zur Dokumentation und Überprüfung seiner technischen und organisatorischen Maßnahmen.

1 Maßnahmen zur Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

2 Maßnahmen zur Gewährleistung der Vertraulichkeit

2.1 Zutrittskontrolle

Die Zutrittskontrolle bezieht sich auf den räumlichen Schutz der Datenverarbeitungsanlagen. Unbefugten Dritten ist durch bauliche, technische und personelle Maßnahmen der Zutritt zu den Räumlichkeiten, in denen sich Datenverarbeitungsanlagen und personenbezogene Daten befinden, zu verwehren.

Die Maßnahmen lassen sich Sicherheitsbereichen zuordnen. Räumlichkeiten, in denen keine sensiblen Daten verarbeitet werden, unterfallen dabei dem Sicherheitsbereich 1.

Werden in bestimmten Abschnitten des Bürogebäudes sensible Daten verarbeitet, sind diese Bereiche einer höheren Sicherheitsstufe (Sicherheitsstufe 2) zuzuordnen. Das Rechenzentrum hat die Sicherheitsstufe 3, da hier der gesamte Datenbestand und das Backup verortet sind.

2.1.1 Situation beim IQTIG

Das IQTIG hat anhand der getroffenen Erwägungen ein Zutrittskonzept erstellt.

Die Geschäftsräume des IQTIG befinden sich auf der fünften, achten und (ab 2018) sechsten Etage eines Bürogebäudes, das auch von anderen Firmen genutzt wird. Dem IQTIG steht jedoch

ein räumlich abgetrennter Bereich zur Verfügung, der von den anderen dort ansässigen Firmen getrennt ist. Im Geschäftsgebäude befinden sich die Mitarbeiterbüros des IQTIG und Datenverarbeitungsgeräte wie Personal-Computer und Laptops.

Der gesamte Bürobereich ist unterteilt in zwei Sicherheitszonen. Empfang und Konferenzräume sind der Sicherheitszone 1 zugeordnet. Hier werden grundsätzlich keine Qualitätssicherungsdaten aufbewahrt. In der Sicherheitszone 2 befinden sich die Mitarbeiterbüros. Hier werden die Datenverarbeitungsanlagen aufbewahrt. Besucher haben hier in der Regel keinen Zutritt, anderenfalls werden sie von einer Mitarbeiterin oder einem Mitarbeiter des IQTIG begleitet.

Getrennt von diesen Räumlichkeiten hat das IQTIG einen Serverraum in einem Rechenzentrum angemietet (Sicherheitszone 3). Das Rechenzentrum ist ISO 27001, ISO 90011 und ISO 14001 zertifiziert und verfügt über ein eigenes Sicherheitskonzept, welches vom IQTIG vorab überprüft wurde und in regelmäßigen Abständen kontrolliert wird.

2.1.2 Im Einzelnen getroffene Maßnahmen

Das IQTIG hat im Einzelnen folgende Schutzmaßnahmen getroffen:

2.1.2.1 Räumlichkeiten des IQTIG (Sicherheitszone 1 und 2)

Zum Zutrittsschutz der Räumlichkeiten des IQTIG wurden die folgenden Maßnahmen getroffen:

- Der Zutritt zu den Räumlichkeiten des IQTIG ist nur unter Verwendung eines Transponder-Chips möglich.
- Die Ausgabe des Transponder-Chips erfolgt nur an die Mitarbeiter des IQTIG und wird von der Personalabteilung dokumentiert.
- Bei Beendigung des Arbeitsverhältnisses ist der Transponder-Chip abzugeben. Dies wird dokumentiert.
- Die Mitarbeiter sind dazu angehalten, den Verlust des Transponder-Chips unverzüglich zu melden. Nach Verlustmeldung wird der Chip gesperrt.
- Der Transponder-Chip ist äußerlich neutral gestaltet. Damit wird im Falle des Chipverlusts verhindert, dass unbefugte Dritte eine Zuordnung zum IQTIG treffen können.
- Besucher müssen sich am Empfang anmelden und registrieren.
- In den Eingangsbereichen sind nur Türen eingebaut, die besonders gegen Einbruch gesichert sind.
- Ein besonderer Einbruchsschutz der Fenster ist nicht erforderlich, da sich die Geschäftsräume in der fünften, achten und (ab 2018) sechsten Etage befinden und die Fenster auch nicht von Unbefugten von außen, beispielsweise über eine Feuerleiter, erreichbar sind.
- Der Haupteingangsbereich im Erdgeschoss des Gebäudes ist mit einem Portier besetzt (24/7). Es gibt feste Öffnungs- und Schließzeiten. In den Schließzeiten ist es ohne Transponder-Chip nicht mehr möglich, über den regulären Eingang zu den Räumlichkeiten des IQTIG zu gelangen.
- Zusätzlich wird der Haupteingangsbereich des Gebäudes durch eine Videokamera über Monitore überwacht.

2.1.2.2 Räumlichkeiten des IQTIG (Sicherheitsstufe 2)

- Durch die Aufteilung in zwei Sicherheitsbereiche haben Besucher zunächst nur Zutritt zum Empfangsbereich und zu den Konferenzräumen. Die Mitarbeiterbüros sind durch eine weitere zugangsgesicherte Tür abgetrennt.
- Besucher dürfen sich nur unter der Begleitung eines autorisierten Mitarbeiters in den Räumlichkeiten des IQTIG bewegen.
- Das Büro der Systemadministratoren ist zusätzlich mit einer separat codierten Schließanlage, deren Code nur den zutrittsberechtigten Mitarbeitern (z. B. Systemadministratoren) bekannt ist, gesichert.

2.1.2.3 Räumlichkeiten des Rechenzentrums (Sicherheitsstufe 3)

- Der Eingang zum Rechenzentrum ist durch einen 24/7 Portier besetzt. Auch außerhalb der regulären Geschäftszeiten wird ein gleich hohes, stetiges Sicherheitsniveau gewährleistet.
- Zutritt zu den Räumlichkeiten des Rechenzentrums haben ausschließlich die Systemadministratoren. Sie müssen dem Rechenzentrum als zutrittsberechtigt schriftlich angezeigt werden.
- Zutrittsberechtigte Mitarbeiter (Systemadministratoren) erhalten nur nach einer Identitätskontrolle durch die Vorlage des Personalausweises Einlass.
- Lieferanten ist der Zutritt zum Rechenzentrum untersagt. Ware muss in einem Vorraum abgestellt werden.
- Besucher (Wartungs-Dienstleister) dürfen ausschließlich in Begleitung eines zutrittsberechtigten Mitarbeiters und nach vorheriger Authentisierung im Rechenzentrum den Serverraum betreten.
- Der Eingangsbereich wird zusätzlich videoüberwacht.
- Die einzelnen Racks sind gesondert abgeschlossen.

2.2 Zugangskontrolle zum IT-System des IQTIG

Der Zugang ist als Eindringen in das Datenverarbeitungssystem selbst zu verstehen. Durch die hier getroffenen Maßnahmen soll verhindert werden, dass unberechtigte Dritte Zugang zur Hard- und Software erhalten und so die Möglichkeit haben, Daten wahrzunehmen, zu entwenden, zu verändern oder zu löschen.

Der Prozess der Zugangskontrolle besteht aus der Identifikation des Nutzers, die Prüfung der Berechtigung (Authentifikation) und der Einrichtung technischer Sicherheitsmaßnahmen bei fehlerhaften Anmeldeversuchen.

2.2.1 Situation beim IQTIG

Der Zugang zu den Datenverarbeitungsanlagen des IQTIG ist nur nach Passworteingabe möglich. Zur Gewährleistung der erforderlichen Passwortsicherheit hat das IQTIG in einer Passwortrichtlinie Vorgaben definiert, die von den Mitarbeiterinnen und Mitarbeitern umzusetzen sind. Außerdem stellt das IQTIG den Zugangsschutz auch durch technische Maßnahmen sicher. Die nachfolgenden Maßnahmen gelten auch für den Umgang mit mobilen Endgeräten (Laptops/Smartphones).

2.2.2 Im Einzelnen getroffene Maßnahmen

Das IQTIG hat im Einzelnen die folgenden Maßnahmen getroffen:

2.2.2.1 Technischer Zugangsschutz

- Nutzer (Mitarbeiterinnen, Mitarbeiter und berechtigte Dritte) müssen sich über die Eingabe eines Nutzernamens und Passworts authentifizieren.
- Die Authentifizierung ist notwendig für den Zugang auf das jeweilige Betriebssystem, für die Herstellung einer VPN-Verbindung und für den Zugriff auf die Datenbanken.
- Die zur Passwortsicherheit getroffenen Vorgaben werden, sofern möglich, durch folgende technische Maßnahmen umgesetzt
 - Eine Kennwortänderung wird nach Ablauf von 90 Tagen technisch erzwungen.
 - Die Wahl von Trivialpasswörtern wird verhindert.
 - Das Passwort wird bei der Eingabe durch Platzhalter angezeigt.
 - Beim Passwortwechsel ist die Wiederholung der letzten 24 Passwörter ausgeschlossen. Das neue Passwort muss sich von dem vorherigen um mindestens drei Zeichen unterscheiden.
 - Passwörter werden nur verschlüsselt gespeichert.
 - Nach zehn Fehlversuchen wird die Benutzererkennung gesperrt. Eine Freigabe kann nur durch den Systemadministrator veranlasst werden.
 - Erfolgreiche und nicht erfolgreiche Login-Versuche werden protokolliert.
 - Systemseitig ist ein passwortgeschützter Bildschirmschoner eingerichtet, der nach zehn Minuten Abwesenheit automatisch aktiviert wird.
 - Der E-Mail Web Access ist https verschlüsselt (257 Bit-Verschlüsselung).
 - Das Netzwerk ist durch eine Firewall vor Eindringen Dritter von außen geschützt.

2.2.2.2 Organisatorischer Zugangsschutz

Die Anforderungen an die Passwortsicherheit sind in einer Passwort-Richtlinie (s. Anlage 4 des DSK) vorgegeben. Die Passwort-Richtlinie enthält folgende Regelungen:

- Die Verwendung von Trivialpasswörtern ist verboten. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- Innerhalb des Passworts muss mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Das Passwort muss mindestens sieben Zeichen lang sein.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) werden durch individuelle Passwörter ersetzt.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Passwörter müssen geheim gehalten werden und dürfen nur dem Benutzer persönlich bekannt sein.
- Das Passwort muss regelmäßig gewechselt werden.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt wurde oder der Verdacht hierfür besteht.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.

- Die Eingabe des Passworts muss unbeobachtet stattfinden.
- Administratoren sind zur Geheimhaltung der Kennwörter verpflichtet.
- Der Wechsel eines „organisatorischen“ Passworts beim Ausscheiden eines zuständigen Mitarbeiters wird durch „on- und offboarding Regelungen“ sichergestellt.
- Es finden regelmäßige Schulungen zum sicheren Umgang mit Passwörtern statt.
- Das Passwort eines Nutzers wird bei längerer Abwesenheit (ab 3 Monate) gesperrt.

2.3 Zugriffskontrolle

Die Zugriffskontrolle stellt sicher, dass Mitarbeiterinnen, Mitarbeiter und befugte Dritte nur im Rahmen ihrer Rechte auf Daten zugreifen, sie lesen, kopieren, ändern oder entfernen können. Die Rechtevergabe richtet sich dabei nach dem konkreten Aufgabenbereich der Mitarbeiterin und des Mitarbeiters (Need-To-Know-Prinzip).

2.3.1 Umsetzung beim IQTIG

Das IQTIG setzt die Zugriffskontrolle überwiegend durch ein differenziertes Berechtigungskonzept um. Die Rollenvergabe erfolgt dabei nach den Aufgabenbereichen der Mitarbeiterinnen und der Mitarbeiter.

2.3.2 Im Einzelnen getroffene Maßnahmen

Das IQTIG hat im Einzelnen die folgenden Maßnahmen getroffen:

2.3.2.1 Technische Maßnahmen

- Mitarbeiterinnen und Mitarbeiter haben nur Zugriff auf Daten entsprechend ihrer Berechtigung.
- Der Zugriff auf das Netzwerk ist von außen nur mittels eines VPN-Zugangs und mittels zertifizierter Hardware des IQTIG möglich.
- Administratoren haben neben dem Admin-Account auch einen eigenen Benutzer-Account. Dadurch ist eine deutliche Trennung zwischen ihren administrativen Aufgaben und nicht-administrativen Aufgaben möglich.

2.3.2.2 Organisatorische Maßnahmen

- Das IQTIG stellt bis Oktober 2018 ein differenziertes Rollen- und Berechtigungskonzept auf und realisiert dies im Routinebetrieb. Dabei ist sichergestellt, dass Mitarbeiterinnen und Mitarbeiter nur in dem Umfang Zugriff auf Daten haben, den sie für ihre jeweilige Aufgabenerledigung benötigen. Je nach Aufgabenbereich können Mitarbeiterinnen und Mitarbeiter die Aktionen „Lesen“, „Schreiben“ oder „Ändern“ vornehmen. Benötigt eine Mitarbeiterin oder ein Mitarbeiter eine weitergehende Berechtigung, muss diese zuvor von der Abteilungsleitung genehmigt werden.
- Bei Eintritt einer neuen Mitarbeiterin oder eines neuen Mitarbeiters, bei Wechsel der Abteilung oder beim endgültigen Ausscheiden aus dem Arbeitsverhältnis existiert ein Prozess für die Einrichtung und Entziehen von Berechtigungen.
- Die IT-Abteilung wird über den Eintritt, Austritt oder Funktionswechsel einer Mitarbeiterin oder eines Mitarbeiters rechtzeitig informiert.

- Die Mitarbeiterinnen und Mitarbeiter haben zusätzlich die ausdrückliche Arbeitsanweisung, Qualitätssicherungsdaten nur innerhalb der Verfahren in ihrem Zuständigkeitsbereich auszuwerten.

2.4 Trennungsgebot

Das Trennungsgebot soll gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Nicht verlangt wird hingegen eine räumliche Trennung, durch die Daten in gesonderten Systemen oder Datenträgern gespeichert werden.

2.4.1 Situation beim IQTIG

Beim IQTIG werden die zu unterschiedlichen Zwecken erhobenen Daten in getrennten Datenbanken gespeichert. Die Qualitätssicherungsdaten werden in eigenen Datenbanken verwaltet.

2.5 Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den jeweiligen Weisungen des G-BA verarbeitet werden.

2.5.1 Situation beim IQTIG

Das IQTIG ist auf Grundlage der Vereinbarung zur Regelung der Rahmenbedingungen für die Beauftragung insbesondere im Sinne von § 137a Abs. 3 SGB V im Aufgabenbereich der Qualitätssicherung im Verhältnis zum G-BA Auftragnehmer. Die inhaltlichen Vorgaben an die Beauftragung ergeben sich für das IQTIG aus den Richtlinien und Beschlüssen des G-BA.

3 Maßnahmen zur Gewährleistung der Integrität

3.1 Weitergabekontrolle

Durch die Weitergabekontrolle soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

3.1.1 Situation beim IQTIG

Das IQTIG ist aufgrund des Gesetzes in besonderer Weise dazu verpflichtet, Qualitätssicherungsdaten nur verschlüsselt zu übertragen. Das Verschlüsselungsverfahren kann sich dabei zwischen den jeweiligen QS-Verfahren unterscheiden. Eine einheitliche Darstellung ist daher nicht möglich. Details zur Verschlüsselung sind den Verfahrensrichtlinien zu entnehmen.

3.1.2 Im Einzelnen getroffene Maßnahmen:

3.1.2.1 Technische Maßnahmen

- Der Transfer der Qualitätssicherungsdaten zwischen den Beteiligten erfolgt verschlüsselt. Das Verschlüsselungsverfahren ist der jeweiligen Spezifikation der QS-Verfahren zu entnehmen.
- Sensible Daten werden auf externen Datenträgern und Laptops nur in verschlüsselten Bereichen gespeichert.

3.1.2.2 Organisatorische Maßnahmen

- Für die Verfahren der Qualitätssicherung wurden unterschiedliche Verschlüsselungstechniken entwickelt.
- Die Verschlüsselungsverfahren entsprechen den Maßgaben des Bundesamts für Sicherheit in der Informationstechnik.
- Die Übermittlung verschlüsselter Dokumente von den Leistungserbringern an das IQTIG wird für jedes Verfahren detailliert spezifiziert.
- In der IT-Richtlinie ist geregelt, dass USB-Sticks grundsätzlich zu verschlüsseln sind. Eine Ausnahme besteht nur bei weniger sensiblen Daten, wie beispielsweise Präsentationen.
- Es dürfen nur externe Datenträger verwendet werden, die vom IQTIG hierfür angeschafft wurden.
- Die IT-Richtlinie enthält Vorgaben zum sicheren Transport von Daten und Datenträgern. Diese dürfen nur in verschlossenen Behältern transportiert und dürfen nicht unbeaufsichtigt gelassen werden.

3.2 Eingabekontrolle

Die Eingabekontrolle verpflichtet das IQTIG zu gewährleisten, dass nachvollzogen werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht wurden.

3.2.1 Situation beim IQTIG

Beim IQTIG werden beim Betrieb von IT-Systemen die Anforderungen an die Protokollierung im Rahmen des technisch Möglichen und Zumutbaren umgesetzt.

3.3 Im Einzelnen getroffene Maßnahmen:

- Folgende Maßnahmen werden protokolliert:
 - Hoch- und Herunterfahren von zentralen Rechnern (v. a. Servern und Firewalls)
 - Aufruf von Administrations-Tools
 - Einrichten, Ändern, Löschen von Benutzern
 - Verwalten von Befugnistabellen
 - Benutzung von automatisierten Abrufverfahren
 - Erfolgreiche und nicht erfolgreiche Login-Versuche
 - Passwortänderungen

- Die Protokolldaten werden über einen Zeitraum von sechs Monaten gespeichert, so dass bei Auffälligkeiten eine Durchsicht der Protokolle erfolgen kann.
- Die Protokolldaten sind ausreichend vor Manipulation gesichert. Ausschließlich Administratoren haben Zugriff auf die Logfiles
- Logging von Maßnahmen in der Teilnehmerverwaltung

4 Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle / Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Ziel der Verfügbarkeitskontrolle ist der Schutz der Daten vor zufälliger Zerstörung der Datenverarbeitungsanlagen. Systeme müssen außerdem die Fähigkeit besitzen, mit risikobedingten Veränderungen umgehen zu können, und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

4.1.1 Situation beim IQTIG

Das IQTIG hält die Qualitätssicherungsdaten und das Backup in einem durch einen externen Dienstleister betriebenen Rechenzentrum vor sowie eine Kopie zur Wiederherstellung von Systemen auf einem verschlüsselten Datenträger im IQTIG im Sicherheitsbereich 2.

4.2 Im Einzelnen getroffene Maßnahmen:

- Es erfolgt eine regelmäßige Sicherung für die auf den Servern laufenden Systeme. Es werden folgende Sicherungen vorgenommen: täglich, wöchentlich und monatlich.
- Das Backup wird in einem anderen Brandabschnitt gelagert als das Produktivsystem.
- Es werden regelmäßige Testläufe zur Datenwiederherstellung durchgeführt.
- Die Serverräume sind besonders gegen Brand gesichert (Brandfrüherkennungsanlage, CO2 Löschanlage, feuerfester Doppelboden).
- Die Serverräume sind klimatisiert.
- Die Serverräume und Netzwerkanbindungen sind mit einer unterbrechungsfreien Stromversorgung (USV) ausgestattet.
- Es gibt einen Stromgenerator (Dieselgenerator), der im Notfall anspringt, um einen Ausfall der Systeme zu verhindern.
- Ein Intrusion-Prevention-System ist vorhanden.

5 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen zu implementieren.

5.1 Situation beim IQTIG

- Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten
- Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen
- Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt
- Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).

Anlage 2

IT Datenschutzmaßnahmen im IQTIG

1 Zutrittskontrolle

1.1 Colt RZ

Die gesamte Server- und Storagehardware des IQTIG steht in gemieteten Serverschränken beim Rechenzentrumsanbieter Colt. Das Colt RZ hat eine Zertifizierung nach ISO 27001. Es werden folgende Maßnahmen getroffen um den Zutritt für Unbefugte zu verhindern:

- Wachschutz
- Videoüberwachung
- Chipkartenleser an den Türen
- Alarmanlagen

1.2 IQTIG Standort am Katharina-Heinroth-Ufer

Der Serverraum des IQTIG ist durch ein Codeschloss geschützt. Die Datenunterverteilungen (Netzwerkschränke) befinden sich in Räumen, die durch Sicherheitsschlösser geschützt sind.

2 Zugangskontrolle

2.1 Zugang zu Computern

Der Zugang zu den Computern erfordert eine Authentifizierung via Passwort. Die Kennwortrichtlinie für die Benutzeraccounts sieht wie folgt aus:

Das Kennwort muss:

- aus mindestens 7 Zeichen bestehen
- mindestens einen Buchstaben in Großschreibung enthalten
- mindestens einen Buchstaben in Kleinschreibung enthalten
- mindestens 1 Zahl enthalten

Kennwortgültigkeit:

- 90 Tage

Kennworthistorie:

- die letzten 24 Kennwörter können nicht erneut verwendet werden

Kontosperrungsschwelle:

- Nach 10 nicht erfolgreichen Anmeldeversuchen wird das Benutzerkonto gesperrt und muss vom Admin entsperrt werden.

3 Zugriffskontrolle

3.1 Berechtigungen auf dem Dateiserver

Die Berechtigungen auf dem (Windows-)Dateiserver werden mithilfe der NTFS-Berechtigungen gesetzt. Diese werden aktuell noch von den Admins mit Windows Bordmitteln gesetzt. In Zukunft wird dies mit der Rechtemanagementsoftware Tenfold in dafür definierten Workflows erledigt werden.

3.2 Benutzererkennung mit Passwort

Alle Serverdienste, Zugriffe auf Netzwerkkomponenten und Zugriffe auf die Firewall erfolgen mit einem Benutzer und einem Kennwort. Die Passwörter werden in einer Passwortdatenbank in der Software „KeePass“ gespeichert und auf dem Dateiserver abgelegt.

3.3 USB-Schnittstelle

Die USB-Schnittstellen der Computer sind mithilfe der Software „Sophos Endpoint Security an Control“ eingeschränkt. Die Software erlaubt das Sperren der USB Schnittstelle, den Vollzugriff oder die Leseberechtigung. Außerdem können Ausnahmen mithilfe von Geräte-IDs definiert werden. Hier gibt eine Whitelist mit zugelassenen (verschlüsselten) USB-Sticks.

3.4 CD/DVD Laufwerk

Der Zugriff auf CD/DVD Laufwerke ist eingeschränkt. Es wird, wie bereits in 3.3. erwähnt, dieselbe Software zur Regulierung des Zugriffs auf die optischen Laufwerke eingesetzt.

3.5 Netzwerk-Schnittstelle

Der Zugang zum Netzwerk wird mithilfe von VLANs (Virtual Local Area Network) geregelt. Das Netzwerk wurde hierbei in mehrere virtuelle LAN-Segmente aufgeteilt um die verschiedenen IP-Netze im IQTIG voneinander zu trennen.

3.6 WiFi Hotspot

Das IQTIG stellt ein offenes WLAN für Gäste zur Verfügung. Das WLAN Netzwerk wird von der Sophos UTM bereitgestellt. Die Sophos Access Points sorgen dafür, dass die Empfangsqualität an allen Stellen im Institut ausreichend gut ist. Das Passwort für den Gäste Hotspot Login wird täglich von der Sophos UTM neu generiert und vom Empfang an Gäste verteilt.

3.7 Office-Makros

Alle eingehenden E-Mail-Anhänge mit Office-Makros (.docm, .xlsm, .pptm usw.) werden durch den SMTP Proxy auf der Sophos UTM gelöscht. Office-Makros sind im Institut außerdem via Richtlinie gesperrt. Die Dokumente können in einer geschützten Ansicht geöffnet werden. Das Bearbeiten oder Ausführen der Makros ist nicht möglich.

Um Ausnahmen zu definieren werden von den Admins sog. „Trusted Folders“ definiert, in denen das Ausführen von Makro-Dokumenten gestattet ist. Diese Ordner sind Zugriffsbeschränkt. I.d.R hat nur die Person, die die Makros ausführen muss das Recht auf den jeweiligen Ordner.

4 Weitergabekontrolle

4.1 Verschlüsselung von Endgeräten

Zur Verschlüsselung der Notebooks wird aktuell die Bitlocker Laufwerksverschlüsselung von Microsoft genutzt. Sie hat den Vorteil, dass sie in Windows integriert ist und ohne Zusatzsoftware aktiviert werden kann. Es wird eine Vollschlüsselung der gesamten Festplatte mit einem AES-256 Bit Schlüssel eingesetzt. Derzeit sind noch nicht alle Notebooks verschlüsselt. Daran wird momentan gearbeitet.

4.2 Verschlüsselung von Wechseldatenträgern

USB-Sticks werden grundsätzlich mit Bitlocker vollverschlüsselt. Zum Entschlüsseln ist ein Kennwort und ein Windows Computer nötig.

4.3 VPN-Zugang

Der VPN-Zugang zum IQTIG wird mithilfe der Sophos UTM Firewall realisiert. Die Sophos UTM bietet dafür eine personalisierte OpenVPN Clientsoftware für Windows und MacOS. Der Benutzer wird von den Admins eingerichtet und die Software kann vom User über das via SSL gesicherte Sophos Userportal heruntergeladen werden. Das VPN-Netz ist über eine in die Sophos UTM integrierte Firewall geschützt. Entsprechende Firewall-Regeln sorgen dafür, dass bestimmte Services aus dem VPN-Netz genutzt werden können (z.B. Zugriff auf Dateiserver oder Outlook).

4.4 Sicherung beim Transport (SSL-Verschlüsselung)

Bei der Übermittlung von elektronischen Daten zwischen Client und Server wird SSL-Verschlüsselung eingesetzt. Dies gilt für alle Webserver, die von Extern erreichbar sind. Für die internen Webserver wurde dies noch nicht auf allen Servern umgesetzt. Das öffentliche Zertifikat wird von der D-Trust GmbH ausgestellt und nutzt eine SHA-256 RSA Verschlüsselung.

4.5 E-Mail AntiSpam/AntiVirus/Sender Blacklists

Da die Sophos UTM als SMTP Proxy jede E-Mail prüft dient sie als AntiSpam und AntiVirus Lösung für eingehende und ausgehende Mails von/nach Extern. Spam-Mails werden hierbei anhand von Mustern identifiziert und in die Quarantäne verschoben. Die Sophos UTM bedient sich außerdem an den gängigen öffentlichen Blacklists um bereits bekannte Spam-Mail-Sender zu blockieren.

5 Verfügbarkeitskontrolle

5.1 Unterbrechungsfreie Stromversorgung

Zur unterbrechungsfreien Stromversorgung werden im Katharina-Heinroth-Ufer entsprechende Online-USV Geräte der Marke AEG eingesetzt. Im Colt RZ wird dies vom Rechenzentrumsanbieter übernommen. Die Server und Storages werden über 2 verschiedene Phasen abgesichert. Ein Dieselgenerator sorgt für die Notstromversorgung im Falle eines Stromausfalls.

5.2 RAID Festplattenspiegelung

Um Datenverlust beim Ausfall von Festplatten zu vermeiden wird auf dem Storagesystem ein Festplatten-RAID eingesetzt. Es kommen RAID6 und RAID5 zum Einsatz. Hierbei werden je nach Wichtigkeit der Daten verschiedene Anzahlen an Paritätsfestplatten genutzt.

5.3 Backupkonzept

Das Backup im IQTIG wird nach der 3-2-1 Regel umgesetzt. Die Daten stehen in 3-facher Kopie zur Verfügung. Die Produktivumgebung stellt den Primärspeicher dar, das Veeam VMWare Backup dient als Hauptbackup und die Off-Site-Kopie liegt auf einem Archivsystem der Firma Fast-LTA. Primärspeicher und Backup liegen auf Servern/Storages im Colt RZ. Die Off-Site-Kopie liegt im Serverraum am Katharina-Heinroth-Ufer. Als Backupmedien werden per SAS angebundene Festplatten-RAID-Systeme genutzt. Die Off-Site Kopie wird mittels SMB-Freigabe auf das Archivsystem übertragen. Im Archivsystem liegen sog. „Bricks“, die als Offline-Instanz in einem Safe verwahrt werden können.

5.4 Virenschutzkonzept

Der Virenschutz auf den IT-Systemen wird durch die Software „Sophos Endpoint Security and Control“ gewährleistet. Die Software bietet gängige Funktionen wie:

- On-Access Scan
- Exploit Abwehr zur Bekämpfung von Ransomware
- Firewall
- Application Control
- Data Control um Data Loss Prevention zu gewährleisten
- Device Control zum Sperren von optischen Datenträgern und USB-Sticks
- WebControl zur Filterung des Internetdatenverkehrs

Anlage 3

Passwort-Richtlinie

§ 1 Geltungsbereich

- (1) Diese Richtlinie regelt die Gestaltung und Handhabung von Passwörtern, die zur Authentifizierung berechtigter Benutzer eingesetzt werden. Für administrative Passworte gilt eine gesonderte Richtlinie.
- (2) Sie ist im Rahmen der technischen Möglichkeiten auf alle IT-Systeme und Telekommunikationssysteme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.

§ 2 Pflichten der Benutzer

- (1) Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt oder unverschlüsselt auf Rechnern gespeichert werden.
- (2) Die Länge der Passwörter richtet sich nach dem Schutzbedarf der Daten und Ressourcen. Sie beträgt mindestens sieben Stellen. Benutzerkennungen mit besonderen Rechten und Aufgaben (z. B. Sicherheitsfunktionen oder Anwendungen mit sensiblen Daten) sind mit Passwörtern zu schützen, die mindestens zehn Zeichen umfassen.
- (3) Passwörter sollen technisch so komplex wie möglich zusammengesetzt sein (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). Dies ist der wesentlichste Schutz vor systematischem Ausspähen.
- (4) Passwörter sollen mindestens einen Buchstaben in Großschreibung, mindestens einen Buchstaben in Kleinschreibung und mindestens eine Zahl enthalten.
- (5) Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:
 1. Zeichenwiederholungen
 2. Zahlen und Daten aus dem Lebensbereich des Benutzers
 3. Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen
 4. einfache Ziffern- und Buchstabenkombinationen
 5. Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden
 6. Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter)
- (6) Passwörter sind nach einer dem Schutzbedarf der Daten und Ressourcen angemessenen Frist, mangels weitergehender Bestimmungen spätestens nach 90 Tagen, zu wechseln.
- (7) Passwörter dürfen in der Regel höchstens einmal am Tag gewechselt werden. Sie sind jedoch unverzüglich zu wechseln, wenn der Verdacht besteht, dass sie Dritten bekannt geworden sein könnten.

- (8) Einstiegs- und Übergangspasswörter sind unverzüglich durch eigene Passwörter zu ersetzen.
- (9) Endgeräte sind mit passwortgeschützten Bildschirmschonern bzw. Bildschirmabschaltungen zu versehen, die je nach Schutzwürdigkeit der Daten und Ressourcen nach einer bestimmten Zeit den Zugriff auf das angemeldete Endgerät verhindern. Für die Entsperrung mittels Passwort gelten die Regeln dieser Richtlinie entsprechend.

§ 3 Pflichten der Systemverwaltung und Programmentwicklung

- (1) Passwortdateien sind vor unbefugtem Zugriff zu schützen.
- (2) Bei der Softwareinstallation automatisch vergebene Passwörter sind unverzüglich durch neue zu ersetzen.
- (3) Passwörter, die nicht im Zusammenhang mit dem Anmelden (Login) einzugeben sind (anwendungsbezogene Passwörter), orientieren sich hinsichtlich der Länge der verwendeten Zeichen und der Frist für einen Passwortwechsel am Schutzbedarf der Anwendung und der zu verarbeitenden Daten. Besteht kein zusätzlicher Schutzbedarf, kann von den Vorgaben nach § 2 Absätze 3 bis 5 abgewichen werden.
- (4) Software ist so zu gestalten bzw. grundsätzlich so zu konfigurieren, dass Benutzer nur Passwörter mit einer Mindestlänge von 7 Zeichen vergeben können. Vorgaben für anwendungsbezogene Passwörter haben den jeweiligen Schutzbedarf der Anwendung zu beachten.
- (5) Fehlversuche bei der Passwordeingabe sind zu protokollieren. Die Protokolle sollen regelmäßig ausgewertet werden, um Angriffe und Missbrauch aufzudecken.
- (6) Soweit möglich, ist durch softwaretechnische Maßnahmen vorzugeben, dass
 1. nur Passwörter vergeben werden können, die aus der größtmöglichen Zeichenmischung von Groß- und Kleinbuchstaben sowie Ziffern zusammengesetzt sind,
 2. nach der vorgegebenen Frist, spätestens nach 180 Tagen, ein Passwortwechsel erzwungen wird,
 3. neue Benutzerkennungen, die länger als 45 Tage nicht aktiviert wurden, gesperrt werden,
 4. Passwörter nicht am Bildschirm angezeigt werden,
 5. Passwörter nach aktuellem Stand der Technik einwegverschlüsselt gespeichert werden,
 6. nach 10-maliger fehlerhafter Passwordeingabe die Benutzerkennung gesperrt wird,
 7. Passwörter in Netzwerken verschlüsselt übertragen werden und
 8. leicht zu erratende Passwörter nicht vergeben werden können
 9. die letzten 24 Kennwörter nicht erneut verwendet werden können.
- (7) Ist die Sperrung der betroffenen Benutzerkennungen nach 10-maliger fehlerhafter Passwordeingabe nicht möglich oder sinnvoll, sind andere gleichwertige Maßnahmen zu treffen (z. B. Zeitverzögerungen zwischen den möglichen Eingabeversuchen).
- (8) Bei der Auswahl von IT-Systemen ist auf die Verfügbarkeit entsprechender Mechanismen zu achten. Sofern diese auf Ebene der Betriebssysteme oder der Anwendung nicht verfügbar sind, ist der Einsatz geeigneter Zusatz-Software erforderlich.

§ 4 Pflichten der für die Passwortverwaltung Zuständigen

- (1) Sollte Passwortrücksetzung erforderlich sein, so hat diese über einen Auftragsberechtigten zu erfolgen. Dabei hebt auf Antrag eines Berechtigten die für die Passwortverwaltung zuständige Stelle die Sperre einer Benutzerkennung auf oder neutralisiert ein Benutzerpasswort, wenn sie sich von der Identität des Berechtigten überzeugt hat. Wurde die Sperre einer Benutzerkennung von einem zur Autorisierung von Benutzern Berechtigten verfügt, darf die Passwortverwaltung sie nur auf dessen Auftrag hin zurücknehmen.
- (2) Das Aufheben der Sperre und die Passwortneutralisierung sind revisionssicher zu dokumentieren, so dass nachvollziehbar ist, wer der Auftraggeber war und wie seine Berechtigung und Identität geprüft wurde.
- (3) Ein von der Passwortverwaltung vergebenes Übergangspasswort (z. B. bei der Entsperrung oder der Passwortneutralisierung) ist so mitzuteilen, dass eine Kenntnisnahme durch Unbefugte vermieden wird. Zugleich ist der Empfänger des Übergangspasswortes aufzufordern, das Übergangspasswort unverzüglich zu ändern.
- (4) Der Inhaber der Benutzerkennung ist von einer Passwortneutralisierung zu informieren, wenn sie nicht von ihm veranlasst wurde. Zugleich ist der Inhaber aufzufordern, das neutralisierte Passwort unverzüglich zu ändern.
- (5) Nicht mehr benötigte oder für einen längeren Zeitraum nicht genutzte Kennungen sind zu sperren, außer es ist für die Funktionsfähigkeit des Betriebes als solchen notwendig, dass die Kennung nicht gesperrt werden kann. Dies gilt auch für entsprechende Wartungs- und Fernwartungskennungen.

§ 5 Organisatorische Maßnahmen

- (1) Soweit der Schutzbedarf der Daten und Ressourcen es erfordert, sind für die Passwörter eine angemessene Länge von mindestens 10 Stellen und eine kürzere Gültigkeitsdauer als 90 Tage festzulegen. Bei der Festlegung der angemessenen Gültigkeitsdauer sind insbesondere der potentielle Schaden zu berücksichtigen, der entstände, wenn ein Unbefugter das Passwort über einen längeren Zeitraum nutzen würde, sowie das Risiko, das ein Unbefugter das Passwort noch längere Zeit nach Kenntnisnahme nutzen könnte.
- (2) Die Einhaltung dieser Richtlinie ist durch geeignete Maßnahmen sicherzustellen.
- (3) Die Beschäftigten sind entsprechend den über den Inhalt dieser Richtlinie zu informieren.

§ 6 Sonstige Maßnahmen

- (1) Benutzerkennungen sollen personenbezogen vergeben werden.
- (2) Werden andere Authentisierungsmittel als Passwörter eingesetzt (z. B. Magnet- bzw. Chip-Karte, Token), müssen sie so gehandhabt werden, dass die Benutzung durch Unbefugte ausgeschlossen ist. Soweit erforderlich, treffen die zuständigen Stellen hierzu besondere Regelungen.

§ 7 Ausnahmeregelungen

Die Institutsleitung kann Ausnahmegenehmigungen von dieser Richtlinie erteilen, wenn die Grundsätze des Datenschutzes und der Datensicherheit eingehalten werden und keine Gefahr für die IT- Infrastruktur besteht. Dabei sind insbesondere die Verfahrensbeschreibung und die Risikoanalyse anzupassen, sowie der Datenschutzbeauftragte des IQTIG zu beteiligen.

Anlage 4

IT Nutzungs-Richtlinie

Verpflichtung zur Datensicherheit und zur verantwortungsbewussten und kostenbewussten Nutzung der informationstechnischen Einrichtungen des IQTIG

Präambel

Die Sicherheit des IQTIG ist in hohem Maße vom fehlerfreien Funktionieren der technischen Einrichtungen, speziell auch der informationstechnischen Einrichtungen abhängig. Dazu gehören die elektronische Datenverarbeitung (EDV) und die Telefonanlage. Durch Computerviren, Spionage und Sabotage sind diese Einrichtungen besonders gefährdet. Unsachgemäße Nutzung, bewusster und unbewusster Missbrauch der informationstechnischen Einrichtungen gefährden diese nicht nur, sie verursachen auch erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung. Selbstverständlich müssen laut Datenschutzgesetz personenbezogene Daten von Patientinnen und Patienten, Leistungserbringern, Kostenträgern, Mitarbeiterinnen und Mitarbeitern der Trägerorganisationen, des G-BA und des IQTIG selbst sowie von Lieferanten besonders geschützt werden.

Um die Sicherheit und den Schutz der informationstechnischen Einrichtungen und der gespeicherten Daten zu gewährleisten und die Kosten der Informationstechnologie in akzeptablen Grenzen zu halten, ist es notwendig, dass alle Mitarbeiterinnen und Mitarbeiter des IQTIG mit den informationstechnischen Einrichtungen verantwortungsbewusst und kostenbewusst umgehen. Die nachfolgend aufgeführten Richtlinien sind von allen Mitarbeiterinnen und Mitarbeitern einzuhalten.

1 Verwendung und Installation von Software

1. Im EDV-Netzwerk des IQTIG und besonders auf allen Servern, Computern und Laptops dürfen nur Softwareprodukte installiert und genutzt werden, die von der Institutsleitung bzw. von der Leitung der Abteilung Informationstechnologie (IT) genehmigt wurden und die rechtmäßig lizenziert wurden. Ausnahmen von dieser Regelung (z. B. der Testbetrieb neuer Software oder aktualisierter Softwareversionen) bedürfen der Genehmigung der IT-Leitung.

2. Die Installation von Software darf ausschließlich durch Personen erfolgen, die durch die Institutsleitung damit beauftragt wurden. Insbesondere gelten folgende Regelungen:
 - Betriebssysteme, Anwendungsprogramme, Updates und Hotfixes dürfen nur von Beauftragten der Institutsleitung (Systemadministration) installiert werden.
 - Softwareentwicklerinnen und Softwareentwickler können nach schriftlicher Genehmigung durch die IT-Leitung lokale Administrationsrechte auf ihren Arbeitsplatzrechnern erhalten, um den Download und die Installation von Software für ihre Entwicklungsarbeit zu ermöglichen. Der Download und die Installation sind vor der tatsächlichen Durchführung schriftlich mit der IT- Leitung abzustimmen.
 - Mitarbeiterinnen und Mitarbeiter dürfen ohne Befugnis keine fremde Software aus dem Internet herunterladen oder auf anderem Weg auf Computern des IQTIG installieren oder transferieren. Dazu gehören auch Bildschirmschoner, Demoprogramme, Apps, Computerspiele oder Utilities.
 - Ohne besondere Genehmigung (in der Regel durch die Systemadministration) dürfen keine fremden Programme direkt aus dem Internet oder aus E-Mail-Anhängen gestartet werden. Die Benutzung von Memory-Sticks, USB-Laufwerken, Bluetooth- oder anderen Verbindungen zur Übertragung von Datenbeständen, die von außerhalb des Firmengeländes kommen, ist untersagt und wird über Gruppenrichtlinien verhindert. Eine Sondergenehmigung kann für Mitarbeiterinnen und Mitarbeiter erteilt werden, die einen Austausch von Daten mit Dritten regelmäßig benötigen. Diese wird schriftlich und mit Beschränkung auf den notwendigen Arbeitsbereich von der Institutsleitung und nach Information der IT-Abteilung erteilt.
 - Alle Datenbestände, die von außerhalb des Firmengeländes (z. B. auf externen Datenträgern wie externen Festplatten, Disketten, CDs, DVDs, Memory-Sticks, USB-Laufwerken etc.) kommen, müssen durch das aktuelle Antivirenprogramm des IQTIG überprüft werden, bevor sie verwendet werden.
3. Ausschließlich dazu befugte Personen dürfen von gekaufter oder von im IQTIG selbst erstellter Software Kopien erstellen oder Dritten übergeben. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.
4. Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Notiz in den Büros der Mitarbeiterinnen und Mitarbeiter noch als unverschlüsselte Datei auf Computern oder Datenträgern. Wichtige administrative Passwörter müssen in einem versiegelten Umschlag im Tresor des IQTIG hinterlegt werden. Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden. Es gilt die Passwort-Richtlinie des IQTIG.

2 Verwendung und Schutz der Daten

5. IQTIG-interne Daten dürfen nur mit Genehmigung der Institutsleitung außerhalb des IQTIG verwendet werden. Insbesondere dürfen ohne Zustimmung der Institutsleitung interne Datenbestände, speziell personenbezogene oder Produktdaten, weder mittels

- E-Mail oder Fax noch mittels anderer Datenträger (Laptop, Diskette, CD, DVD, Memory-Stick, USB-Laufwerke, externe Festplatte etc.) oder in ausgedruckter Form außer Haus gebracht werden, sofern sie nicht außerhalb des IQTIG für dienstliche Zwecke benötigt werden.
6. Sofern IQTIG-interne Daten außerhalb des IQTIG verwendet werden, müssen diese auf durch entsprechende Software verschlüsselten und mit Passwort geschützten Datenträgern/Laufwerken oder Verzeichnissen gespeichert werden. Die Geräte, auf die diese Daten zu dienstlichen Zwecken übertragen wurden, sind vor dem Zugriff Dritter zu schützen und dürfen nicht unbeobachtet gelassen werden. Dateien, die ausdrücklich für den Austausch mit Dritten vorgesehen sind (z. B. Präsentationen), dürfen auf unverschlüsselten Datenträgern (z. B. Memory-Sticks) Dritten (auch per E-Mail) zur Verfügung gestellt werden.
 7. Die Mitarbeiterin/der Mitarbeiter sichert zu, dass sie/er alle ihm im Rahmen des Vertragsverhältnisses und ihrer/seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten des IQTIG, seiner Mitarbeiterinnen und Mitarbeiter, Lieferanten und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Arbeitsverhältnisses hinaus, streng vertraulich behandelt und geheim hält. Sie/er versichert, dass sie/er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung ihrer/seiner Dienstpflichten. Zieht das IQTIG Dritte zur Mitarbeit hinzu, wird diesen die gleiche Verschwiegenheitspflicht auferlegt.
 8. Die Mitarbeiterin/der Mitarbeiter darf nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für sie/ihn und ihr/sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist die Vorgesetzte/der Vorgesetzte oder die EDV-Abteilung ohne Verzug zu informieren.
 9. Mitarbeiterinnen und Mitarbeiter, denen von der Institutsleitung und der IT-Leitung ein Zugriff auf die Bereiche des LANs oder WANs des IQTIG mithilfe einer VPN-Verbindung schriftlich erlaubt wurde, dürfen diese nur von Geräten aus nutzen, die ihnen vom IQTIG hierfür zur Verfügung gestellt wurden.
 10. Mitarbeiterinnen und Mitarbeiter, die mit der Datensicherung beauftragt sind, haben diese Aufgaben mit besonderer Sorgfalt durchzuführen und müssen andere Vorgesetzte bzw. die IT-Leitung unverzüglich informieren, wenn Probleme aufgetreten sind oder Gefahr im Verzug ist.
 11. Betriebsdaten müssen generell so gespeichert werden, dass bei Ausfall einer Mitarbeiterin oder eines Mitarbeiters deren/dessen Vertretung oder die/der Vorgesetzte auf diese Daten zugreifen kann. Für die Speicherung von Betriebsdaten ist das persönliche Verzeichnis, auf das nur die einzelne Mitarbeiterin oder der einzelne Mitarbeiter über ihr/sein Passwort zugreifen kann, nicht zugelassen. Betriebsdaten wie Word- oder Excel-Dateien sollten vielmehr in Gruppenverzeichnissen abgelegt werden. Damit bei Ausfall

einer Mitarbeiterin oder eines Mitarbeiters diese Daten von anderen Mitarbeiterinnen und Mitarbeitern gefunden werden, muss die Ordnerstruktur im Gruppenverzeichnis auf dem/den Server/n ständig mit den zuständigen Kolleginnen und Kollegen abgesprochen oder an eindeutiger, allgemein auffindbarer Stelle dokumentiert werden. Namen für Ordner oder Dokumente sollen eindeutig gemäß den Namenskonventionen des IQTIG gewählt werden, damit Dokumente auch von Kolleginnen und Kollegen schnell geortet werden können.

12. Ordner- und Dateinamen sowie die eindeutige Identifizierung von Dateiversionen unterliegen den IQTIG-spezifischen Vorgaben, die einzuhalten sind.
13. Verlässt eine Mitarbeiterin oder ein Mitarbeiter befristet (z. B. Mutterschaftsurlaub, Elternzeit, Kur) oder unbefristet (Kündigung, Rente) das IQTIG, so ist sie/er angehalten, die eigenen Datenbestände an eine Kollegin oder einen Kollegen zu übergeben und dies zu dokumentieren. Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.
14. Für die verschlüsselte Übertragung von Mails und für die verschlüsselte Kommunikation mit den Webportalen des IQTIG gelten folgende Regelungen:
 - Termine und Kontakte dürfen mit privaten Handys synchronisiert werden. Dabei ist zu berücksichtigen, dass der Eintrag im Kalender bei Terminen, die datenschutzrechtlich schützenswert sind (bei besonderem und gerechtfertigtem Interesse einer der beteiligten Personen an der Geheimhaltung entsprechender Aktivitäten), so zu gestalten ist, dass dem Schutzbedürfnis Rechnung getragen wird.
 - Mails dürfen nicht auf privaten Handys abgerufen oder mit diesen synchronisiert werden.
 - Auf Diensthandys gilt keine Einschränkung, es dürfen also Kontakte, Termine und E-Mails synchronisiert werden.
 - Die Nutzung von Webmail (verschlüsselter Mailverkehr) ist auch von privaten Geräten aus gestattet.

3 Störungen und Defekte, Verstöße gegen diese Richtlinien

15. Bei Verdacht auf Virengefahr, Datenspionage oder andere Umstände, die die Sicherheit der Informationstechnologie des IQTIG betreffen, sind unverzüglich eine Vorgesetzte/ein Vorgesetzter und die Leitung der Abteilung Informationstechnologie des IQTIG zu informieren.
16. Störungen und Defekte bei informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich den dafür zuständigen Personen zu berichten.

17. Jede Mitarbeiterin und jeder Mitarbeiter ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchsmaterialien.
18. Da die Arbeit des IQTIG in hohem Maße von der Funktionsfähigkeit der informationstechnischen Einrichtungen abhängig ist, kann ein grob fahrlässiger oder vorsätzlicher Verstoß gegen eine oder mehrere der vorgenannten Regeln zu einer Beendigung des Beschäftigungsverhältnisses aus wichtigem Grund führen, ohne dass es einer zusätzlichen Abmahnung bedarf.
19. Ferner haftet diejenige Mitarbeiterin oder derjenige Mitarbeiter, die/der gegen die genannten Regeln verstößt, zivilrechtlich für die dadurch entstehenden Schäden nach den gesetzlichen Regeln.

Anlage 5

Verzeichnis von Verfahrenstätigkeiten

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Indirekte Verfahren nach QSKH-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software, R (Statistiksoftware)
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Annahme und Auswertung von Daten zur Qualitätssicherung gemäß QSKH-RL des G-BA
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

Indirekte Verfahren nach QSKH-RL

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Weitergabe der zusammengeführten Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten
Art der gespeicherten Daten bzw. Datenkategorien:	Pseudonymisierte Gesundheitsdaten, die im Rahmen der QSKH-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden.
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Daten von Leistungserbringern über Datenannahmestellen und eine Vertrauensstelle)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie, Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Landesgeschäftsstellen nach QSKH-RL des G-BA

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des DUS-, QIAW- und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der Daten richten sich nach den Vorgaben der QSKH-RL.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten könnten durch Diebstahl sowie die Ermittlung des dazugehörigen Patienten z. B. durch Einbruch beim leistungserbringenden Krankenhaus und Einsichtnahme in die Software, die die Vorgangsnummern in den Datensätzen den Patienten-IDs im Krankenhaus zuweist, einer Person zugeordnet werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Follow-up Verfahren nach QSKH-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software, R (Statistiksoftware)
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Zusammenführung von Datensätzen über Patientenpseudonyme oder ET-Nummern zur Follow-up-Betrachtung im Rahmen der Zweckangaben der externen Qualitätssicherung nach QSKH-RL des G-BA.
Zweckänderung: (optionale Angabe)	

Follow-up Verfahren nach QSKH-RL

Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Weitergabe der zusammengeführten Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant. Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten
Art der gespeicherten Daten bzw. Datenkategorien:	Pseudonymisierte Gesundheitsdaten, die im Rahmen der QSKH-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden.
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Daten von Leistungserbringern über Datenannahmestellen und eine Vertrauensstelle)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie, Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Landesgeschäftsstellen nach QSKH-RL des G-BA

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des DUS-, QIAW- und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der Daten richten sich nach den Vorgaben der QSKH-RL.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	<p>Die Daten mit den Patientenpseudonymen könnten durch Diebstahl und weitere Maßnahmen (Diebstahl des Geheimnisses/Algorithmus bei der Vertrauensstelle oder Entwicklung einer technischen Möglichkeit der Rückführung der Pseudonyme auf die eGK-Nummer eines Patienten) sowie die Ermittlung des dazugehörigen Patienten z. B. durch Diebstahl der Karte oder Einbruch beim Arzt oder der Krankenkasse direkt dem Patienten zugeordnet werden.</p> <p>Die Zuordnung einer ET-Nummer kann nach Diebstahl der Daten sowie Einbruch beim Leistungserbringer, Eurotransplant, der DSO oder einem klinischen Transplantationsregister einer Person zugeordnet werden.</p>

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Direkte Verfahren nach QSKH-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software, R (Statistiksoftware)
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Annahme und Auswertung von Daten zur Qualitätssicherung gemäß QSKH-RL des G-BA sowie Teilnehmerverwaltung
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Weitergabe der zusammengeführten Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten, Ansprechpartner bei Leistungserbringern
Art der gespeicherten Daten bzw. Datenkategorien:	Pseudonymisierte Gesundheitsdaten, die im Rahmen der QSKH-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden. Kontaktdaten von Ansprechpartnern bei Leistungserbringern
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Daten von Leistungserbringern)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Ansprechpartner der Leistungserbringer

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des DUS-, QIAW- und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der personenbezogenen Daten richten sich nach den Vorgaben der QSKH-RL. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die QS-Daten könnten durch Diebstahl sowie die Ermittlung des dazugehörigen Patienten z. B. durch Einbruch beim leistungserbringenden Krankenhaus und Einsichtnahme in die Software, die die Vorgangsnummern in den Datensätzen den Patienten-IDs im Krankenhaus zuweist, einer Person zugeordnet werden. Die Daten der Ansprechpartner können durch Diebstahl direkt ermittelt werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Datenübermittlung zum Qualitätsbericht
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software, R (Statistiksoftware)
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Datenexport für aggregierte QS-Ergebnisse von Leistungserbringern der Direkten Verfahren gem. QSKH-RL und zu Verfahren der plan.QI-RL des G-BA zum Zwecke der „Information, Orientierungs- und Entscheidungshilfe für alle interessierten Personen, z.B. für Patienten und Patientinnen sowie Leistungserbringer“ gemäß Zielsetzung in § 1 der Qb-R des G-BA

Datenübermittlung zum Qualitätsbericht

Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Übertragung der Daten erfolgt unverschlüsselt per E-Mail gem. Vorgaben der Qb-R des G-BA. Sie sind aggregiert und dadurch anonymisiert. Das Verfahren wurde durch die BfDI in einem Stellungnahmeverfahren datenschutzrechtlich geprüft und genehmigt. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant. Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Betroffene Personengruppen sind die den errechneten Ergebnissen zugrundeliegenden Patienten, die dem IQTIG jedoch nur in anonymisierter oder pseudonymisierter Weise zugestellt werden.
Art der gespeicherten Daten bzw. Datenkategorien:	Ergebnisse von Qualitätssicherungsdaten
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten von einem Dritten (Daten von Leistungserbringern)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	ITSG (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH)

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des DUS-, QIAW- und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung zum Qualitätsbericht

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschfristen der dem Ergebnisexport zugrundeliegenden Daten richten sich nach den Vorgaben der QSKH-RL und der plan.QI-RL.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Das verbleibende Risiko ist, dass die gesendeten Daten mit einem nicht maskierten Ergebnis <4 abgefangen werden und der Datendieb durch Recherchen in der Region des zugehörigen Krankenhauses ermittelt, welche Person eine Erkrankung aus dem QS-Verfahren hat.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Bericht zum strukturierten Dialog
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Software zur Entgegennahme der Daten des Strukturierten Dialoges der Firma Unitrend
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Erstellung von Übersichten zu Ergebnissen des Strukturierten Dialoges auf Bundesebene gemäß QSKH-RL; Teilnehmerverwaltung
Zweckänderung: (optionale Angabe)	

Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b) Einwilligung (Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit a)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Übertragung der Daten erfolgt verschlüsselt, die Daten des Strukturierten Dialoges der Landesebene enthalten keinen Personenbezug. Die Daten werden jedoch von Ansprechpartnern der Landesgeschäftsstellen für Qualitätssicherung, übermittelt, die beim IQTIG registriert werden. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle und die Regelungen aus den Verträgen zur Auftragsdatenverarbeitung relevant. Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt.

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Ansprechpartner bei den Landesgeschäftsstellen für Qualitätssicherung (LQS)
Art der gespeicherten Daten bzw. Datenkategorien:	Adressdaten von Ansprechpartnern der LQS
Herkunft der Daten:	Von den Landesgeschäftsstellen für Qualitätssicherung (LQS)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Softwareentwickler des DUS-, und Online-Dienste Teams, Verfahrenssupport, fachlich verantwortliche Mitarbeiter im Verfahrensmanagement, Systemadministratoren, Mitarbeiter von Unitrend mit unterzeichneter Vertraulichkeitserklärung
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	Firma Unitrend GmbH Am Elsterberg 19 99094 Erfurt Fax: 0361 / 653 198 49
Schriftlicher datenschutzkonformer Vertrag	Ja
Geeignetheit des Auftragsverarbeiters	Ja
Standort der Verarbeitung	Berlin (IQTIG)

Bericht zum strukturierten Dialog

--	--

Datenübermittlung in Drittstaaten / internationale Organisationen

Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten

Speicherdauer	Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten der Ansprechpartner können durch Diebstahl direkt ermittelt werden.

Stellungnahme des Datenschutzbeauftragten

Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung

Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Datenvalidierung nach QSKH-RL und plan. QI-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Software zur Entgegennahme der Daten der Datenvalidierung der Firma Unitrend
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Erstellung von Übersichten zur Datenqualität auf Bundesebene gemäß QSKH-RL und plan.QI-RL; Ermittlung von Daten aus Patientenakten zur Überprüfung der Datenqualität gemäß QSKH-RL und plan.QI-RL; Teilnehmerverwaltung
Zweckänderung: (optionale Angabe)	

Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Daten werden zwischen den Ansprechpartnern der Landesgeschäftsstellen für Qualitätssicherung sowie des MDK ausgetauscht. Diese sind beim IQTIG registriert. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle und die Regelungen aus den Verträgen zur Auftragsdatenverarbeitung relevant. Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten; Ansprechpartner bei den Landesgeschäftsstellen für Qualitätssicherung (LQS)
Art der gespeicherten Daten bzw. Datenkategorien:	Gesundheitsdaten, die im Rahmen der QSKH-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden; Adressdaten von Ansprechpartnern der LQS und des MDK
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Leistungserbringer); Von den Landesgeschäftsstellen für Qualitätssicherung (LQS); Vom MDK

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Landesgeschäftsstellen für Qualitätssicherung (LQS); MDK

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Softwareentwickler des DUS-, und Online-Dienste Teams, Verfahrenssupport, fachlich verantwortliche Mitarbeiter im Verfahrensmanagement, Systemadministratoren, Mitarbeiter von Unitrend mit unterzeichneter Vertraulichkeitserklärung
Nachweis	Active-Directory, Berechtigungskonzept

Datenvalidierung nach QSKH-RL und plan. QI-RL

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	Firma Unitrend GmbH Am Elsterberg 19 99094 Erfurt Fax: 0361 / 653 198 49
Schriftlicher datenschutzkonformer Vertrag	Ja
Geeignetheit des Auftragsverarbeiters	Ja
Standort der Verarbeitung	Berlin (IQTIG)

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten der Ansprechpartner können durch Diebstahl direkt ermittelt werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Verfahren nach plan. QI-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Annahme und Auswertung von Daten zur Qualitätssicherung gemäß QSKH-RL und plan. QI-RL des G-BA
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

Verfahren nach plan. QI-RL

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle und die Regelungen aus den Verträgen zur Auftragsdatenverarbeitung relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten; Zuweiser*innen, (nach)behandelnde Ärzt*innen, Ansprechpartner bei den Landesgeschäftsstellen für Qualitätssicherung (LQS), Vertreter von Landesplanungsbehörden, Vertreter von Landesverbänden der Krankenkassen/Ersatzkassen
Art der gespeicherten Daten bzw. Datenkategorien:	Gesundheitsdaten, die im Rahmen der plan. QI-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden; Adressdaten von Ansprechpartnern der LQS, Vertretern von Landesplanungsbehörden, Vertretern von Landesverbänden der Krankenkassen/Ersatzkassen
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Leistungserbringer); Von den Landesgeschäftsstellen für Qualitätssicherung (LQS)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement, Verfahrensentwicklung, Fachbereich Biometrie
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Landesgeschäftsstellen für Qualitätssicherung (LQS); Landesplanungsbehörden

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Softwareentwickler des DUS-, und Online-Dienste Teams, Verfahrenssupport, fachlich verantwortliche Mitarbeiter im Verfahrensmanagement, im Fachbereich Biometrie und in der Verfahrensentwicklung Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	

Verfahren nach plan. QI-RL

Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der QS-Daten richten sich nach den Vorgaben der QSKH-RL und der plan. QI-RL. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten der Ansprechpartner können durch Diebstahl direkt ermittelt werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	QS-Verfahren nach DeQS-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Zusammenführung von Datensätzen über Patientenpseudonyme zur Follow-up-Betrachtung im Rahmen der Zweckangaben der externen Qualitätssicherung nach DeQS-RL des G-BA.
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

QS-Verfahren nach DeQS-RL

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten
Art der gespeicherten Daten bzw. Datenkategorien:	Gesundheitsdaten, die im Rahmen der DeQS-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden; Sozialdaten bei den Krankenkassen mit Bezug zu den QS-Verfahren der DeQS-RL des G-BA
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Daten von Leistungserbringern und Krankenkassen über Datenannahmestellen und eine Vertrauensstelle)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Landesarbeitsgemeinschaften und übergangsweise Kassen(zahn)ärztliche Vereinigungen und LQS nach DeQS-RL

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des DUS-, QIAW- und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der Daten richten sich nach den Vorgaben der DeQS-RL.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten der Ansprechpartner können durch Diebstahl direkt ermittelt werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Verfahren nach QSD-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Zusammenführung von Datensätzen über Patientenpseudonyme zur Follow-up-Betrachtung im Rahmen der Zweckangaben der externen Qualitätssicherung nach QSD-RL des G-BA.
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

Verfahren nach QSD-RL

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Personenidentifikatoren sind gemäß Richtlinie des G-BA anonymisiert bzw. pseudonymisiert. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten
Art der gespeicherten Daten bzw. Datenkategorien:	Gesundheitsdaten, die im Rahmen der QSD-RL des G-BA zum Zweck der Qualitätssicherung erhoben werden
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten und ggf. patientenidentifizierenden Daten von einem Dritten (Daten von Leistungserbringern über Datenannahmestellen, Berichtersteller und eine Vertrauensstelle)

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie, Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Kassenärztliche Vereinigungen nach QSD-RL

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des DUS-, QIAW- und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der Daten richten sich nach den Vorgaben der QSD-RL.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten mit den Patientenpseudonymen könnten durch Diebstahl und weitere Maßnahmen (Diebstahl des Geheimnisses/Algorithmus bei der Vertrauensstelle oder Entwicklung einer technischen Möglichkeit der Rückführung der Pseudonyme auf die eGK-Nummer eines Patienten) sowie die Ermittlung des dazugehörigen Patienten z. B. durch Diebstahl der Karte oder Einbruch beim Arzt oder der Krankenkasse direkt dem Patienten zugeordnet werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Risikostatistik nach QSKH-RL und DeQS-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Software zur Entgegennahme der Sollstatistik der Fa. Unitrend
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Erstellung von Dokumentationsraten gem. QSKH-RL und DeQS-RL Teilnehmerverwaltung
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Risikostatistikdaten enthalten keinen Personenbezug. Die Daten werden jedoch von Ansprechpartnern der Landesgeschäftsstellen für Qualitätssicherung (LQS) übermittelt, die beim IQTIG registriert werden. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle und die Regelungen aus den Verträgen zur Auftragsdatenverarbeitung relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Ansprechpartner bei den LQS
Art der gespeicherten Daten bzw. Datenkategorien:	Kontaktdaten der Ansprechpartner bei den LQS
Herkunft der Daten:	Von den Ansprechpartnern bei der LQS

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Kassenärztliche Vereinigungen nach QSD-RL

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Softwareentwickler des DUS-, und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren, Mitarbeiter von Unitrend mit unterzeichneter Vertraulichkeitserklärung
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	Firma Unitrend GmbH Am Elsterberg 19 99094 Erfurt Fax: 0361 / 653 198 49
Schriftlicher datenschutzkonformer Vertrag	Ja
Geeignetheit des Auftragsverarbeiters	Ja
Standort der Verarbeitung	Berlin (IQTIG)

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der Daten richten sich nach den Vorgaben der DeQS-RL. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten mit den Patientenpseudonymen könnten durch Diebstahl und weitere Maßnahmen (Diebstahl des Geheimnisses/Algorithmus bei der Vertrauensstelle oder Entwicklung einer technischen Möglichkeit der Rückführung der Pseudonyme auf die eGK-Nummer eines Patienten) sowie die Ermittlung des dazugehörigen Patienten z. B. durch Diebstahl der Karte oder Einbruch beim Arzt oder der Krankenkasse direkt dem Patienten zugeordnet werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Sollstatistik nach QSKH-RL und DeQS-RL
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Software zur Entgegennahme der Sollstatistik der Fa. Unitrend
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Erstellung von Dokumentationsraten gem. QSKH-RL und DeQS-RL Teilnehmerverwaltung
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt, die Sollstatistikdaten enthalten keinen Personenbezug. Die Daten werden jedoch von Ansprechpartnern der Landesgeschäftsstellen für Qualitätssicherung (LQS), Kassenärztlichen Vereinigungen oder der Datenannahmestelle für selektivvertraglich tätige Einrichtungen übermittelt, die beim IQTIG registriert werden. Die Übermittlung der Daten ist durch gesetzliche und untergesetzliche Vorgaben geregelt.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle und die Regelungen aus den Verträgen zur Auftragsdatenverarbeitung relevant.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Ansprechpartner bei den LQS
Art der gespeicherten Daten bzw. Datenkategorien:	Kontaktdaten der Ansprechpartner bei den LQS
Herkunft der Daten:	Von den Ansprechpartnern bei der LQS

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Softwareentwickler des DUS-, und Online-Dienste Teams, Verfahrenssupport, Systemadministratoren, Mitarbeiter von Unitrend mit unterzeichneter Vertraulichkeitserklärung
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	Firma Unitrend GmbH Am Elsterberg 19 99094 Erfurt Fax: 0361 / 653 198 49
Schriftlicher datenschutzkonformer Vertrag	Ja
Geeignetheit des Auftragsverarbeiters	Ja
Standort der Verarbeitung	Berlin (IQTIG)

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschfristen der Daten richten sich nach den Vorgaben der DeQS-RL. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die Daten mit den Patientenpseudonymen könnten durch Diebstahl und weitere Maßnahmen (Diebstahl des Geheimnisses/Algorithmus bei der Vertrauensstelle oder Entwicklung einer technischen Möglichkeit der Rückführung der Pseudonyme auf die eGK-Nummer eines Patienten) sowie die Ermittlung des dazugehörigen Patienten z. B. durch Diebstahl der Karte oder Einbruch beim Arzt oder der Krankenkasse direkt dem Patienten zugeordnet werden.

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Strukturierter Dialog bzw. Stellungnahmeverfahren
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Der Zweck ergibt sich aus den Vorgaben der QSKH-RL und DeQS-RL des G-BA. Der Strukturierte Dialog (QSKH-RL) bzw. das Stellungnahmeverfahren (plan.QI-RL) dient dazu, einen Leistungserbringer auf Auffälligkeiten aus den Qualitätsbewertungen des IQTIGs hinzuweisen und ihnen eine Möglichkeit zur Stellungnahme zu geben. Zur Erfüllung dieses Zweckes ist eine Allgemeine Teilnehmerverwaltung notwendig, über die der Zugang

Strukturierter Dialog bzw. Stellungnahmeverfahren

	zum Portal für den Strukturierten Dialog bzw. das Stellungnahmeverfahren geregelt wird.
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Übertragung der Daten erfolgt verschlüsselt in einem geschützten Extranet. Der Login erfolgt nach formaler Registrierung zu dem Verfahren unter Verwendung der Zugangsdaten der zentralen Teilnehmerverwaltung. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle relevant sowie die Behandlung von übermittelten Daten, die nicht dem Zwecke des Verfahrens dienen, wie z. B. personenidentifizierende Daten. Über eine Arbeitsanweisung ist geregelt, dass diese umgehend zu löschen sind. Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Ansprechpartner bei den LQS
Art der gespeicherten Daten bzw. Datenkategorien:	Ergebnisse von Qualitätssicherungsdaten; Kontaktdaten von Verantwortlichen eines Krankenhauses
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten von Leistungserbringern über Datenannahmestellen und eine Vertrauensstelle; Ansprechpartner beim Leistungserbringer

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des Online-Dienste Teams, Verfahrenssupport, Systemadministratoren,
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	

Strukturierter Dialog bzw. Stellungnahmeverfahren

Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschrfristen der dem Ergebnisexport zugrundeliegenden Daten richten sich nach den Vorgaben der QSKH-RL und der plan.QI-RL. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	NICU-Verfahren
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Verfahrensgrundlagen / Sozialdaten Günther Heller Guenther.heller@iqtig.org 030/58 58 26 - 450
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Der Zweck ergibt sich aus den Vorgaben der QFR-RL des G-BA. Die Qualitätsdaten können durch den Leistungserbringer bzw. die LQS in das System eingestellt werden. Der klärende Dialog mit einem Krankenhaus bzw. dessen Perinatalzentrum dient dazu, einen Leistungserbringer auf Auffälligkeiten aus den

	<p>Qualitätsbewertungen zu Anforderungen an die pflegerische Versorgung des IQTIGs hinzuweisen und ihnen eine Möglichkeit zur Stellungnahme zu geben.</p> <p>Zur Erfüllung dieses Zweckes ist eine Allgemeine Teilnehmerverwaltung notwendig, über die der Zugang zum Portal geregelt wird.</p>
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Die Übertragung der Daten erfolgt verschlüsselt in einem geschützten Extranet. Der Login erfolgt nach formaler Registrierung zu dem Verfahren unter Verwendung der Zugangsdaten der zentralen Teilnehmerverwaltung.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung sind insbesondere die Zugriffskontrolle relevant sowie die Behandlung von übermittelten Daten, die nicht dem Zwecke des Verfahrens dienen, wie z. B. personenidentifizierende Daten. Über eine Arbeitsanweisung ist geregelt, dass diese umgehend zu löschen sind.</p> <p>Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Registrierte Ansprechpartner der Leistungserbringer und Landesgeschäftsstellen (LQS)
Art der gespeicherten Daten bzw. Datenkategorien:	Ergebnisse von Qualitätssicherungsdaten; Kontaktdaten von Verantwortlichen eines Krankenhauses; vom Leistungserbringer übermittelte Qualitätsdaten
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten von Leistungserbringern über Datenannahmestellen; Ansprechpartner beim Leistungserbringer

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Fachlich verantwortliche Mitarbeiter und Softwareentwickler des Online-Dienste Teams, Verfahrenssupport
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Verantwortliche beim Krankenhaus/Leistungserbringer Ergebnisse des klärenden Dialogs werden aufbereitet für die breite Öffentlichkeit über das Portal http://perinatalzentren.org/ bereitgestellt.

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des Online-Dienste Teams, Verfahrenssupport, Systemadministratoren, Leistungserbringer und Landesgeschäftsstellen (für die relevanten Standorte)
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Löschfristen der dem Ergebnisexport zugrundeliegenden Daten richten sich nach den Vorgaben der QFR-RL. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Leistungserbringer oder der Ansprechpartner selbst.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	DokEx - Dokumentenaustauschportal
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Informationstechnologie Gesine Schäfer-Reimers gesine.schaeferreimers@iqtig.org 030 / 58 58 26 300
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Bereitstellung von Dateien für <ul style="list-style-type: none"> • Mitglieder von Fachgruppen in QS-Verfahren • Den Mitgliedern des G-BA und seiner Gremien • Den Beteiligten an den QS-Verfahren auf der Landesebene (LQS, Landesarbeitsgemeinschaft, Landesplanungsbehörden, Kassenärztlichen Vereinigungen, Datenannahmestellen, Leistungserbringer)

	Zur Erfüllung dieses Zweckes ist eine Allgemeine Teilnehmerverwaltung notwendig, über die der Zugang zum DokEx geregelt wird.
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage §§ 136 ff. SGB V, Richtlinien und Beschlüsse des G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b) Einwilligung (Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit a)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Übertragung der Daten erfolgt verschlüsselt in einem geschützten Extranet. Der Login erfolgt nach formaler Registrierung zu dem Verfahren unter Verwendung der Zugangsdaten der zentralen Teilnehmerverwaltung. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant. Das Risiko wird aufgrund der TOMs als nicht hoch eingeschätzt

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Betroffene Personengruppen sind registrierte Ansprechpartner: <ul style="list-style-type: none"> • MitarbeiterInnen des G-BA • MitarbeiterInnen der Trägerorganisationen des G-BA • PatientenvertreterInnen • MitarbeiterInnen der Landesebene • Kontaktpersonen bei Softwareanbieter • MitarbeiterInnen von Leistungserbringern
Art der gespeicherten Daten bzw. Datenkategorien:	<ul style="list-style-type: none"> • Ergebnisdaten • Vorgangslisten aus den QS-Daten • Stellungnahmen • Berichte • Adressdaten
Herkunft der Daten:	Anonymisierte oder pseudonymisierte QS-Daten von Leistungserbringern über Datenannahmestellen und eine Vertrauensstelle; Kontaktdaten von registrierten Benutzern

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Fachlich verantwortliche Mitarbeiter und Softwareentwickler des Online-Dienste Teams, Verfahrenssupport

Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Registrierte Ansprechpartner, die Inhalte funktionsbezogen einsehen können: <ul style="list-style-type: none"> • MitarbeiterInnen des G-BA • MitarbeiterInnen der Trägerorganisationen des G-BA • PatientenvertreterInnen • MitarbeiterInnen der Landesebene • Softwareanbieter
------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des Online-Dienste Teams, Verfahrenssupport, Systemadministratoren,
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die abgelegten Daten werden maximal drei Jahre vorgehalten. Die Speicherung der Ansprechpartner erfolgt bis auf Widerruf durch den Ansprechpartner.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Lohn- und Gehaltsabrechnung
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Kaufm. Geschäftsführung / Verwaltung Franz-Josef Grothaus franz-josef.grothaus@iqtig.org 030 / 58 58 26 200
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Auftragsverarbeitung
Ort der Verarbeitung: (optionale Angabe)	Deutschland

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	zur Erstellung der Lohnabrechnung; Erfüllung gesetzl. Anforderungen
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7); Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	

Lohn- und Gehaltsabrechnung

Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Es werden Lohn- und Gehaltsdaten einschl. der notwendigen persönlichen Daten (Familienstand, Religion, u.a.) verarbeitet.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der TOMs als nicht hoch eingeschätzt</p>
--------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Erhebung der Daten	
Kreis der betroffenen Personengruppen	<ul style="list-style-type: none"> • Mitarbeiter*innen des IQTIG
Art der gespeicherten Daten bzw. Datenkategorien:	<ul style="list-style-type: none"> • Adressdaten • Bankverbindungsdaten/Kreditkartendaten • Geburtsdatum • Kontaktdaten • Lohn- und Gehaltsdaten • Name/Vorname/Anrede/Titel • Sozialversicherungsdaten • Zahlungsdaten
Herkunft der Daten:	Von den Mitarbeiter*innen selber

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Personalabteilung
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Auftragsverarbeiter

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die verarbeiteten QS-Verfahren und Softwareentwickler des Online-Dienste Teams, Verfahrenssupport, Systemadministratoren,
Nachweis	Active-Directory, Berechtigungskonzept; Datenschutz-/Vertraulichkeitsvereinbarung mit Auftragsdatenverarbeiter

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	Dr. Heilmaier & Partner GmbH Carl-Wilhelm-Straße 16 47798 Krefeld Tel. (02151) 63 90 - 0 Fax (02151) 63 90 - 90
Schriftlicher datenschutzkonformer Vertrag	Nicht notwendig, da Inanspruchnahme fremder Fachleistungen (Steuerberater - s. DSK Kurzpapier Nr. 13 Anhang B)
Geeignetheit des Auftragsverarbeiters	Ja
Standort der Verarbeitung	Deutschland

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	10 Jahre wg. Sozialversicherungs-/Lohnsteuerprüfung
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Bewerbungsmanagement
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Kaufm. Geschäftsführung / Verwaltung Franz-Josef Grothaus franz-josef.grothaus@iqtig.org 030 / 58 58 26 200
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Verwaltung durch Excel-Tabellen und geschützte File-Ablage
Ort der Verarbeitung: (optionale Angabe)	Deutschland

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Zur Ausschreibung der zu besetzenden Stelle, Zur Annahme der Bewerbungen, Auswahl der Einzuladenden, Korrespondenz mit den Bewerber*innen
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Einwilligung bei Aufnahme in den Bewerberpool (Art. 6 Abs. 1 lit. a, Art. 7); Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG)

Bewerbungsmanagement

Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Da es sich um sensible Daten handelt (Name, Alter, Geschlecht, ggf. Religion, Schwerbehinderung u. ä.) sind diese Daten besonders zu schützen.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der TOMs als nicht hoch eingeschätzt</p>

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Bewerber*innen
Art der gespeicherten Daten bzw. Datenkategorien:	<ul style="list-style-type: none"> • Adressdaten • Geburtsdatum • Kontaktdaten • Lohn- und Gehaltsdaten • Name/Vorname/Anrede/Titel • Zahlungsdaten • Standortdaten • Vertragsdaten • Vertragsstammdaten
Herkunft der Daten:	Von den Bewerber*innen selber

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Personalabteilung
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Personalabteilung, Leitungen der Abteilungen, Fachbereiche, Stabsbereiche
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Die Bewerbungsunterlagen aller Bewerber*innen werden bis zu sechs Monate nach Absage aufbewahrt und danach gelöscht, es sei denn, es liegt eine Einwilligung zur Aufnahme in den Bewerberpool vor. Die Daten der eingestellten Person werden bei Abschluss des Arbeitsvertrages in die Personalakte übernommen.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Personaldatenverwaltung
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Kaufm. Geschäftsführung / Verwaltung Franz-Josef Grothaus franz-josef.grothaus@iqtig.org 030 / 58 58 26 200
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Microsoft Excel / BCS
Ort der Verarbeitung: (optionale Angabe)	Deutschland

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Verwaltung der Personalakten
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7); Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	

Personaldatenverwaltung

Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	<p>Da es sich um sensible Daten handelt (Name, Alter, Geschlecht, ggf. Religion, Schwerbehinderung u. ä.) sind diese Daten besonders zu schützen.</p> <p>Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Bei dieser Verarbeitung ist insbesondere die Zugriffskontrolle relevant.</p> <p>Das Risiko wird aufgrund der TOMs als nicht hoch eingeschätzt</p>
--------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Mitarbeiter*innen
Art der gespeicherten Daten bzw. Datenkategorien:	<ul style="list-style-type: none"> • Adressdaten • Geburtsdatum • Kontaktdaten • Lohn- und Gehaltsdaten • Lebenslauf / Bewerbungsunterlagen • Name/Vorname/Anrede/Titel • Sozialversicherungsdaten • Zeiterfassungsdaten
Herkunft der Daten:	Von den Mitarbeiter*innen selber

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Personalabteilung, IT-Abteilung, Buchhaltung, Facility Management
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Sozialversicherungen VBLU – Zusatzrenten Steuerbüro (Lohn- und Gehaltsabrechnung)

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Personalabteilung,
Nachweis	Active-Directory, Berechtigungskonzept;

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	Dr. Heilmaier & Partner GmbH Carl-Wilhelm-Straße 16 47798 Krefeld Tel. (02151) 63 90 - 0 Fax (02151) 63 90 - 90
Schriftlicher datenschutzkonformer Vertrag	Nicht notwendig, da Inanspruchnahme fremder Fachleistungen (Steuerberater - s. DSK Kurzpapier Nr. 13 Anhang B)
Geeignetheit des Auftragsverarbeiters	Ja
Standort der Verarbeitung	Deutschland

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Personalakten werden bis 10 Jahre nach Ausscheiden aus dem Beschäftigungsverhältnis aufbewahrt (Steuerprüfung, Sozialversicherungsprüfung)
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben (Personalakten in verschlossenen Schränken; Elektronische Personaldaten auf geschützten Laufwerken)
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Reisekostenabrechnung
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Kaufm. Geschäftsführung / Verwaltung Franz-Josef Grothaus franz-josef.grothaus@iqtig.org 030 / 58 58 26 200
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	
Ort der Verarbeitung: (optionale Angabe)	Deutschland

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Abrechnung der Reisekosten (intern / extern)
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7); Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	

Reisekostenabrechnung

Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Es werden Name, Adresse, Zahlungsdaten und Reise-/Beschäftigungszeiten erfasst. Das Risiko wird aufgrund der TOMs als nicht hoch eingeschätzt
--------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Mitarbeiter*innen Externe Teilnehmer*innen an Gremiensitzungen
Art der gespeicherten Daten bzw. Datenkategorien:	<ul style="list-style-type: none"> • Adressdaten • Bankverbindungsdaten/Kreditkartendaten • Kontaktdaten • Name/Vorname/Anrede/Titel • Zahlungsdaten
Herkunft der Daten:	Von den Mitarbeiter*innen / Teilnehmer*innen selber

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Personalabteilung, Abt. Verfahrensmanagement, Abt. Verfahrensentwicklung, Finanzbuchhaltung, weitere Abteilungen mit Gremienorganisation
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Personalabteilung, Finanzbuchhaltung
Nachweis	Active-Directory, Berechtigungskonzept;

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Bis zu 10 Jahre wg. Sozialversicherungs-/Lohnsteuerprüfung
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben (Personalakten in verschlossenen Schränken; Elektronische Personaldaten auf geschützten Laufwerken)
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Zeiterfassung Mitarbeiter*innen
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Kaufm. Geschäftsführung / Verwaltung Franz-Josef Grothaus franz-josef.grothaus@iqtig.org 030 / 58 58 26 200
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Betrieb
Art der Verarbeitung / Name der Software: (optionale Angabe)	Zeiterfassungstool in der BCS Projektron Software
Ort der Verarbeitung: (optionale Angabe)	Deutschland

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Kontrolle der Einhaltung arbeitsvertraglicher Vorgaben
Zweckänderung: (optionale Angabe)	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7); Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	

Zeiterfassung Mitarbeiter*innen

Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Da es sich um systematische Bewertung persönlicher Aspekte natürlicher Personen handelt, sind diese Daten besonders zu schützen. - Art. 35 Abs. 3 lit. a) DSGVO. Das Risiko wird aufgrund der TOMs als nicht hoch eingeschätzt
--------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Mitarbeiter*innen
Art der gespeicherten Daten bzw. Datenkategorien:	<ul style="list-style-type: none"> Name/Vorname/Anrede/Titel Zeiterfassungsdaten
Herkunft der Daten:	Von den Mitarbeiter*innen / Teilnehmer*innen selber

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Personalabteilung
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Personalabteilung, Vorgesetzte(r)
Nachweis	Active-Directory, Berechtigungskonzept;

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	
Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten	
Speicherdauer	Bis zu 10 Jahre wg. Sozialversicherungs-/ Lohnsteuerprüfung
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	erfolgt

Zeiterfassung Mitarbeiter*innen

Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

1. Angaben zum Verantwortlichen

Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG)
 Katharina-Heinroth-Ufer 1
 10787 Berlin
 Telefon: 030 / 585826 - 0
 Fax: 030 / 585826 - 999
 eMail: info@iqtig.org
 Internet: www.iqtig.org

Gesetzliche Vertreter (Stand: 03/2018):

Dr. Andreas Gassen -KBV (Vorstandsvorsitzender)
 Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende)
 Johann-Magnus von Stackelberg, GKV-SV (Vorstand)
 Gernot Kiefer - GKV-SV (Vorstand)
 Georg Baum - DKG (Vorstand)
 Dr. Wolfgang Eßer - KZBV (Vorstand)
 StS Lutz Stroppe - BMG (Vorstand)
 Prof. Josef Hecken - G-BA (Vorstand)
 Dr. Christof Veit - Institutsleiter

2. Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

3. Angaben zum Vertreter des Verantwortlichen

4. Angaben zur Person des Datenschutzbeauftragten

Martin Schüller - IQTIG
 eMail: datenschutz@iqtig.org

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

Erstellungsdatum des VVT: 30.08.2018		Datum der letzten Änderung:	
5. Verantwortliche Fachabteilung Fachbereich Wissensmanagement Christiane Rothe 030 / 585826 - 432 christiane.rothe@iqtig.org			
6. Bezeichnung der Verarbeitungstätigkeit Integriertes Bibliothekssystem Koha			
7. Zwecke der Verarbeitung Das Integrierte Bibliothekssystem Koha dient der Abwicklung der medienbezogenen Geschäftsgänge der Bibliothek, insbesondere der Erwerbung und Ausleihe.			
8. Beschreibung der Datenarten sowie der Datenkategorien betroffener Personen		<input checked="" type="checkbox"/> 1 Benutzerdaten - Aktive Benutzer <input checked="" type="checkbox"/> 2 Benutzerdaten - Neuanmeldungen über OPAC-Funktion <input checked="" type="checkbox"/> 3 Benutzerdaten - Änderungsmitteilungen für Adressdaten <input checked="" type="checkbox"/> 4 Benutzerdaten - Gelöscht <input checked="" type="checkbox"/> 5 Benutzersperren <input checked="" type="checkbox"/> 6 Interne und OPAC-Mitteilungen <input type="checkbox"/> 7 Gebühren <input checked="" type="checkbox"/> 8 Vormerkdaten <input checked="" type="checkbox"/> 9 Ausleihdaten <input checked="" type="checkbox"/> 10 Benachrichtigungen <input checked="" type="checkbox"/> 11 Erwerbungsdaten (Benutzer) <input checked="" type="checkbox"/> 12 Zeitschriftenumlauflisten <input type="checkbox"/> 13 Semesterapparaten zugeordnete Dozenten <input checked="" type="checkbox"/> 14 Zugehörigkeit zu einer Benutzerliste <input type="checkbox"/> 15 Zugehörigkeit zu einem Druckauftrag für den Benutzerausweisdruck <input checked="" type="checkbox"/> 16 Daten aus Personalisierungsdiensten <input checked="" type="checkbox"/> 17 Protokolldaten der Bibliotheksmitarbeiter <input checked="" type="checkbox"/> 18 Protokoll- und Statistikdaten - Endnutzer und Bibliotheksbenutzer <input checked="" type="checkbox"/> 19 Sitzungsdaten <input checked="" type="checkbox"/> 20 Entlastungen <input type="checkbox"/> 21 Benutzerfotos <input checked="" type="checkbox"/> 22 Artikelbestellungen <input checked="" type="checkbox"/> 23 Anträge zum Zurücksetzen des Passworts <input checked="" type="checkbox"/> 24 Daten zur Aufsuchenden Bibliotheksarbeit	
9. Rechtsgrundlagen der Verarbeitung (EU-DSGVO, BDSG_neu, LDSG_neu, andere Rechtsvorschriften, Einwilligung)		Vorschrift	Umfang/Art der Verarbeitung
		<input type="checkbox"/> Art. 6 Abs. 1, lit b, f EU-DSGVO (Vertragserfüllung, berechtigtes Interesse)	

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

	<input checked="" type="checkbox"/> § 26 Abs. 1 BDSG-neu (Beschäftigendaten) <input type="checkbox"/> § 4 LDSG BW-Entwurf (Erfüllung der Aufgabe einer öffentlichen Stelle) <input type="checkbox"/> Datenschutzgesetz anderer Bundesländer <input type="checkbox"/> § 12 LHG i. V. mit Hochschul-Datenschutzverordnung <input checked="" type="checkbox"/> Spezielle Rechtsvorschrift, und zwar: Benutzungsordnung der Bibliothek <input checked="" type="checkbox"/> Art. 6 Abs. 1 lit. a EU-DSGVO (Einwilligung) ¹ <input type="checkbox"/> Ggfs. Weitere Rechtsvorschrift, dann bitte benennen
10. Kategorien von Empfängern / Zugriffsberechtigte, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder werden.	<input checked="" type="checkbox"/> intern: Bibliotheksmitarbeitende (Beschäftigte) nach Rollen-/Berechtigungskonzept
	<input checked="" type="checkbox"/> extern: Auftragsverarbeiter <input checked="" type="checkbox"/> Öffentliche Stellen: Supportpersonal des Bibliotheksservice-Zentrum Baden-Württemberg (Konstanz) (Administration) <input type="checkbox"/> Nicht-Öffentliche Stellen: Entfällt

¹ Falls externe Nutzer und Studierende der Speicherung ihrer Daten bei der Anmeldung zustimmen, käme für diesen Nutzerkreis auch 'Einwilligung' in Frage.

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

<p>11. Datenübermittlung an Dritte:</p> <p>Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 EU-DSGVO genannte Datenübermittlung handelt.</p>	<p><input checked="" type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant</p> <p><input type="checkbox"/> Datenübermittlung findet wie folgt statt:</p> <p><input type="checkbox"/> Drittland Name:</p> <p><input type="checkbox"/> Internationale Organisation Bezeichnung:</p> <p><input type="checkbox"/> Nennung des/der konkreten Datenempfänger Name:</p> <p><input type="checkbox"/> Dokumentation geeigneter Garantien:</p>																														
<p>12. Fristen für die Löschung der verschiedenen Datenkategorien²</p>	<table border="1"> <thead> <tr> <th>Datenart</th> <th>Löschfrist [Tage]</th> </tr> </thead> <tbody> <tr> <td>1 Benutzerdaten - Aktive Benutzer</td> <td>Mit Ausscheiden der Mitarbeiter*innen oder bei Widerspruch</td> </tr> <tr> <td>2 Benutzerdaten - Neuanmeldungen über OPAC-Funktion</td> <td>Noch nicht implementiert, geplant für 17.11</td> </tr> <tr> <td>3 Benutzerdaten - Änderungsmitteilungen für Adressdaten</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> <tr> <td>4 Benutzerdaten - Gelöscht</td> <td>Noch nicht implementiert</td> </tr> <tr> <td>5 Benutzersperren</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> <tr> <td>6 Interne und OPAC-Mitteilungen</td> <td>Nicht implementiert</td> </tr> <tr> <td>7 Gebühren</td> <td>Noch nicht implementiert</td> </tr> <tr> <td>8 Vormerkdaten</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> <tr> <td>9 Ausleihdaten</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> <tr> <td>10 Benachrichtigungen</td> <td>Noch nicht implementiert</td> </tr> <tr> <td>11 Erwerbungsdaten (Benutzer)</td> <td>Noch nicht implementiert (s. 4)</td> </tr> <tr> <td>12 Zeitschriftenumlauflisten</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> <tr> <td>13 Semesterapparaten zugeordnete Dozenten</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> <tr> <td>14 Zugehörigkeit zu einer Benutzerliste</td> <td>Mit Löschen der Benutzerdaten (s. 1)</td> </tr> </tbody> </table>	Datenart	Löschfrist [Tage]	1 Benutzerdaten - Aktive Benutzer	Mit Ausscheiden der Mitarbeiter*innen oder bei Widerspruch	2 Benutzerdaten - Neuanmeldungen über OPAC-Funktion	Noch nicht implementiert, geplant für 17.11	3 Benutzerdaten - Änderungsmitteilungen für Adressdaten	Mit Löschen der Benutzerdaten (s. 1)	4 Benutzerdaten - Gelöscht	Noch nicht implementiert	5 Benutzersperren	Mit Löschen der Benutzerdaten (s. 1)	6 Interne und OPAC-Mitteilungen	Nicht implementiert	7 Gebühren	Noch nicht implementiert	8 Vormerkdaten	Mit Löschen der Benutzerdaten (s. 1)	9 Ausleihdaten	Mit Löschen der Benutzerdaten (s. 1)	10 Benachrichtigungen	Noch nicht implementiert	11 Erwerbungsdaten (Benutzer)	Noch nicht implementiert (s. 4)	12 Zeitschriftenumlauflisten	Mit Löschen der Benutzerdaten (s. 1)	13 Semesterapparaten zugeordnete Dozenten	Mit Löschen der Benutzerdaten (s. 1)	14 Zugehörigkeit zu einer Benutzerliste	Mit Löschen der Benutzerdaten (s. 1)
Datenart	Löschfrist [Tage]																														
1 Benutzerdaten - Aktive Benutzer	Mit Ausscheiden der Mitarbeiter*innen oder bei Widerspruch																														
2 Benutzerdaten - Neuanmeldungen über OPAC-Funktion	Noch nicht implementiert, geplant für 17.11																														
3 Benutzerdaten - Änderungsmitteilungen für Adressdaten	Mit Löschen der Benutzerdaten (s. 1)																														
4 Benutzerdaten - Gelöscht	Noch nicht implementiert																														
5 Benutzersperren	Mit Löschen der Benutzerdaten (s. 1)																														
6 Interne und OPAC-Mitteilungen	Nicht implementiert																														
7 Gebühren	Noch nicht implementiert																														
8 Vormerkdaten	Mit Löschen der Benutzerdaten (s. 1)																														
9 Ausleihdaten	Mit Löschen der Benutzerdaten (s. 1)																														
10 Benachrichtigungen	Noch nicht implementiert																														
11 Erwerbungsdaten (Benutzer)	Noch nicht implementiert (s. 4)																														
12 Zeitschriftenumlauflisten	Mit Löschen der Benutzerdaten (s. 1)																														
13 Semesterapparaten zugeordnete Dozenten	Mit Löschen der Benutzerdaten (s. 1)																														
14 Zugehörigkeit zu einer Benutzerliste	Mit Löschen der Benutzerdaten (s. 1)																														

² Die Löschverfahren werden vom BSZ nach Absprache mit der Bibliothek mit ggf. individualisierten Löschfristen eingerichtet. Siehe dazu das Löschkonzept in der vom Verantwortlichen individualisierten Fassung.

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

	15 Zugehörigkeit zu einem Druckauftrag für den Benutzerausweisdruck	Noch nicht implementiert
	16 a) Daten aus Personalisierungsdiensten <ul style="list-style-type: none"> • Sternchenbewertungen • Tagging • Literaturlisten 	Mit Löschen der Benutzerdaten (s.1)
	16 b) <ul style="list-style-type: none"> • Einladungen zum Teilen einer Liste 	Nach 14 Tagen
	16 c) <ul style="list-style-type: none"> • Anmeldungen für automatische Benachrichtigungen 	Noch nicht implementiert
	17 a) Protokolldaten der Bibliotheksmitarbeiter <ul style="list-style-type: none"> • Erstellte Druckaufträge • Erwerbung: Zugriffsberechtigung auf Bestellungen • Erwerbung: Zugriffsberechtigung auf Konten im Haushalt • Ersteller einer Benutzerliste • Ersteller eines Nachrichteneintrags 	Mit Löschen der Benutzerdaten (s. 1)
	17 b) <ul style="list-style-type: none"> • Erwerbung: Ersteller einer Bestellung • Erwerbung: Ersteller eines Kontos im Haushalt • Bearbeiter eines Anschaffungsvorschlags • Ersteller eines Reports • Moderator eines Tags (Social Tagging) 	Noch nicht implementiert (s. 4)
	17 c) <ul style="list-style-type: none"> • Ersteller eines Zeitschriftenabonnements 	Noch nicht implementiert
	18 Protokoll- und Statistikdaten - Endnutzer und Bibliotheksbenutzer	Noch nicht implementiert (s. 4)
	19 Sitzungsdaten	Einmal täglich
	20 Entlastungen	Mit Löschen der Benutzerdaten (s. 1)
	21 Benutzerfotos	Mit Löschen der Benutzerdaten (s. 1)

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

	22 Artikelbestellungen	Mit Löschen der Benutzerdaten (s. 1)
	23 Anträge zum Zurücksetzen des Passworts	Noch nicht implementiert (s. 4)
	24 Daten zur Aufsuchenden Bibliotheksarbeit	Mit Löschen der Benutzerdaten (s. 1)

13. Einschränkung der Verarbeitung (Artikel 4 Abs.3 EU-DSGVO)

14. Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 30 Abs. 2 lit. g und Artikel 32 Abs.1 DSGVO

14.1 Art der eingesetzten DV-Anlagen und Software

14.1.1 Software

Nr.	Art	Software	Version ³	Einsatz
1	Personalarbeitsplatz (Webclient)	Von Koha unterstützte Browser		<input checked="" type="checkbox"/> Client
2	Benutzerarbeitsplatz (Webclient)	Von Koha unterstützte Browser		<input checked="" type="checkbox"/> Client
3	Offline-Verbuchungs-Client	KOCT Firefox Plugin	0.4.13 und höher	<input type="checkbox"/> Client ⁴
4	Betriebssystem	Debian	(old-)stable	<input checked="" type="checkbox"/> Server
5	Webserver	Apache	(old-)stable	<input checked="" type="checkbox"/> Server
6	Datenbankserver	MySQL	(old-)stable	<input checked="" type="checkbox"/> Server
7	Webanwendung	Koha	(old-)stable	<input checked="" type="checkbox"/> Server
8	SIP-Server	Koha	(old-)stable	<input type="checkbox"/> Server ⁵
9	Shibboleth Service Provider	Debian / Koha	(old-)stable	<input type="checkbox"/> Server ⁶
10	LDAP-Client	Koha	(old-)stable	<input type="checkbox"/> Server ⁷

³ Stand bei Erstellung dieses Verzeichnis der Verfahrenstätigkeit (Datum siehe Seite 1)

⁴ Markieren Sie bitte die Checkbox, wenn Sie die Anwendung einsetzen

⁵ Markieren Sie bitte die Checkbox, wenn Sie die Anwendung einsetzen

⁶ Markieren Sie bitte die Checkbox, wenn Sie die Anwendung einsetzen

⁷ Markieren Sie bitte die Checkbox, wenn Sie die Anwendung einsetzen

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

14.1.2 Beteiligte Clients (Workstation, Notebook, Terminal, Videokamera)⁸

Lfd. Nr.	Typ	Betriebssystem Version	Software (lfd. Nr. aus 14.1.1)	Wechselmedien Schnittstellen	Netzwerk-Verbindung	Welche Daten werden lokal gespeichert (lfd. Nr. aus 8)
1	Arbeitsplatz-PCs ohne Offline-Verbuchung	Windows 8 Pro Windows 10 Pro	1, 2	Kartenleser Barcodeleser RFID-Reader	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein	Keine
2	Arbeitsplatz-PCs mit Offline-Verbuchung		1	Kartenleser Barcodeleser RFID-Reader	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein	
3	Selbstverbucher		8	Kartenleser Barcodeleser	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein	
4	Kassenautomat		8	Kartenleser Barcodeleser	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein	

14.1.3 Beteiligte Server (Webserver, Datenbankserver, Proxy-Server)

Lfd. Nr.	Funktion	Betriebssystem Version ⁹	Software (lfd. Nr. aus 14.1.1)	Standort Gebäude, Raum	Gespeicherte Daten (lfd. Nr. aus 8)
1	Anwendungsserver (Produktion)	Debian (old-)stable	4-8	<input checked="" type="checkbox"/> KIM Universität Konstanz Universitätsstr. 10 78464 Konstanz	Alle unter 8 markierten Daten
2 ¹⁰	Anwendungsserver (Test)	Debian (old-)stable	4-8	<input type="checkbox"/> KIM	Alle unter 8 markierten Daten

14.1.4 Backup

Backupsoftware, Version ¹¹	Betriebssystem, Version ¹²	Standort Gebäude, Raum	Gesicherte Daten (lfd. Nr. aus 8)	Backup-Medium	Aufbewahrungs-ort der Backup-Medien
Interne Skripte und Bacula	Vgl. Datensicherungs-Richtlinie des BSZ in der jeweils gültigen Version	<input checked="" type="checkbox"/> KIM	Alle	s. Richtlinie	s. Richtlinie

14.1.5 Verwendete Protokolle und Dienste

Anwendung	Software (lfd. Nr. aus 14.1.1)	Protokoll	Ports
Personalarbeitsplatz (Webclient)	1	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> IPv4 <input type="checkbox"/> UDP <input type="checkbox"/> Sonstige	8080 oder 8082
Benutzerarbeitsplatz (Webclient)	2	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> IPv4 <input type="checkbox"/> UDP <input type="checkbox"/> Sonstige	443

⁸ Bitte Anzahl, Version, Wechselmedien und Schnittstellen für die Windows-Clients ergänzen. Sollten unterschiedliche Klienten vorgesehen sein, ergänzen Sie bitte entsprechende Zeilen analog zur Ersten. Web-Clients müssen hier nicht aufgeführt werden.

⁹ Vgl. Fußnote 3

¹⁰ Markieren Sie bitte die Checkboxes, wenn Sie einen Testserver verwenden.

¹¹ Vgl. Fußnote 3

¹² Vgl. Fußnote 3

Integriertes Bibliothekssystem Koha	Stand: 22.06.18
--------------------------------------------	------------------------

Offline-Verbuchungs-Client	3	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> IPv4 <input type="checkbox"/> UDP <input type="checkbox"/> Sonstige	443
SIP-Server	8	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> IPv4 <input type="checkbox"/> UDP <input type="checkbox"/> Sonstige	22

14.1.6 Verschlüsselung

Übertragungsabschnitt/Anwendung	Verschlüsselungsverfahren	Software (Ifd. Nr. aus 14.1.1)
Browser->Webanwendung	TLS 1.2	7

14.2 Allgemeine technische und organisatorische Maßnahmen (TOM) gemäß Artikel 30 Abs. 2 lit. g und Artikel 32 Abs.1 DSGVO

Erläuterungen zu den einzelnen Maßnahmen, insbesondere soweit diese das Verfahren betreffen, können der jeweils gültigen „Vereinbarung zur Auftragsverarbeitung“ und den zugehörigen „Technischen und organisatorischen Maßnahmen“ entnommen werden.

Dr. Christof Veit
Institutsleiter

.....

Verantwortlicher

Datum

Unterschrift

Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Stiftung für Qualitätssicherung und Transparenz im Gesundheitswesen, (IQTIG) Katharina-Heinroth-Ufer 1, 10787 Berlin
Ggf. gemeinsamer Verantwortlicher	
Gesetzlicher Vertreter (= Geschäftsführung) (Stand: 03/2018)	Dr. Andreas Gassen -KBV (Vorstandsvorsitzender) Dr. Doris Pfeiffer, GKV-SV (stv. Vorstandsvorsitzende) Johann-Magnus von Stackelberg, GKV-SV (Vorstand) Gernot Kiefer - GKV-SV (Vorstand) Georg Baum - DKG (Vorstand) Dr. Wolfgang Eßer - KZBV (Vorstand) StS Lutz Stroppe - BMG (Vorstand) Prof. Josef Hecken - G-BA (Vorstand) Dr. Christof Veit - Institutsleiter
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	
Datenschutzbeauftragter	Martin Schüller - IQTIG

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	Sekundäre Datennutzung
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	Fachbereich Evaluation Dr. Stefan Lhachimi stefan.lhachimi@iqtig.org 030 / 58 58 26 - 4 90
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen	
Status: (optionale Angabe)	In Planung
Art der Verarbeitung / Name der Software: (optionale Angabe)	Eigenentwickelte Software, R (Statistiksoftware)
Ort der Verarbeitung: (optionale Angabe)	Datenverarbeitung und Speicherung auf IQTIG-eigenen Servern im externen Rechenzentrum der Fa. Colt

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Zweckbestimmung:	Auswertung von Daten zur Qualitätssicherung für Zwecke der wissenschaftlichen Forschung und der Weiterentwicklung der Qualitätssicherung auf Antrag eines Dritten
Zweckänderung: (optionale Angabe)	

Sekundäre Datennutzung

Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	Gesetzliche Grundlage § 137a Abs. 10 SGB V, 8. Kapitel VerFO G-BA, Bescheid des G-BA nach § 8 Abs. 2 Satz 1 8. Kapitel VerFO G-BA (Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. b)
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	Die Personenidentifikatoren sind gemäß Richtlinien des G-BA anonymisiert bzw. pseudonymisiert. Die Auswertung der Daten erfolgt ausschließlich im IQTIG. Die Auswertungsergebnisse werden der Antragstellerin oder dem Antragsteller nur anonymisiert und in aggregierter Form zur Verfügung gestellt. Es werden die TOMs gemäß Datenschutzkonzeptes des IQTIG angewandt. Zusätzlich werden spezielle Bedingungen nach Kap. 7.8 des Datenschutzkonzeptes beachtet. Das Risiko wird aufgrund der Richtlinienvorgaben und TOMs als nicht hoch eingeschätzt.

Erhebung der Daten	
Kreis der betroffenen Personengruppen	Patientinnen und Patienten, Antragstellerinnen und Antragsteller
Art der gespeicherten Daten bzw. Datenkategorien:	Pseudonymisierte oder anonymisierte Gesundheitsdaten, Daten von Antragstellerinnen und Antragstellern (Adressdaten, ggf. Bankverbindung)
Herkunft der Daten:	QS-Daten, die im Rahmen der Richtlinien des G-BA zum Zweck der Qualitätssicherung erhoben wurden; Antragsdaten aus Antragsformular

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	Abteilungen Informationstechnologie Verfahrensmanagement und Biometrie, die mit der Bereitstellung, Berechnung und Qualitätssicherung befasst sind. Fachlich verantwortliche Mitarbeiter für die sekundäre Datennutzung.
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	Gemeinsamer Bundesausschuss (Antragsdaten) Antragstellerinnen und Antragsteller (anonyme Auswertungen)

Zugriffsberechtigte Personen (optionale Angaben)	
Zugriffsberechtigte Personen	Fachlich verantwortliche Mitarbeiter für die sekundäre Datennutzung und Softwareentwickler, Datenmanager und Systemadministratoren der Abteilung Informationstechnologie, die zur Bereitstellung der Daten und Analysen sowie zur Administration der technischen Systeme erforderlich sind.
Nachweis	Active-Directory, Berechtigungskonzept

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	
Schriftlicher datenschutzkonformer Vertrag	

Sekundäre Datennutzung

Geeignetheit des Auftragsverarbeiters	
Standort der Verarbeitung	

Datenübermittlung in Drittstaaten / internationale Organisationen

Datenübermittlung in Drittstaaten:	
Drittstaaten / internationale Organisationen	
Angemessenes Datenschutzniveau durch:	

Regelfristen für die Löschung der Daten

Speicherdauer	Die Löschrfristen der personenbezogenen Daten richten sich nach den Vorgaben der Richtlinien des G-BA. Da die Daten der Antragstellerinnen und Antragsteller mit deren Einwilligung durch den G-BA veröffentlicht werden, ist eine Löschrfrist nicht festgelegt.
Nachweis	Löschungen werden in Logfiles dokumentiert

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DS-GVO)	Die TOM sind im Datenschutzkonzept beschrieben
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Die QS-Daten könnten durch Diebstahl sowie die Ermittlung des dazugehörigen Patienten z. B. durch Einbruch im Krankenhaus oder in einer Praxis und Einsichtnahme in die Software, die die Vorgangsnummern in den Datensätzen den Patienten-IDs o. ä. zuweist, einer Person zugeordnet werden. Die Daten der Antragstellerinnen und Antragsteller können durch Diebstahl direkt ermittelt werden. Sie werden jedoch am Ende des Prozesses ohnehin durch den G-BA veröffentlicht.

Stellungnahme des Datenschutzbeauftragten

Prüfung durch den Datenschutzbeauftragten	erfolgt
Besteht weiterer Handlungsbedarf?	nein
Offene Maßnahmen	
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung

Prüfung durch die Geschäftsleitung	
Datum, Unterschrift	

Anlage 6

Richtlinie Betroffenenrechte

1 Einleitung

Am 25.05.2018 ist die Datenschutz-Grundverordnung (nachstehend „DSGVO“) in Kraft getreten. Die DSGVO gewährt betroffenen Personen eine Reihe von Rechten im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten. Durch die gesetzlichen Vorgaben zu den Betroffenenrechten ist die verantwortliche Stelle dazu verpflichtet, ihre Datenverarbeitungsvorgänge gegenüber den betroffenen Personen transparent darzulegen. Den Betroffenen wird damit ein Werkzeug an die Hand gegeben, um die zu ihrer Person gespeicherten Daten auf ihre Richtigkeit zu überprüfen und sich gegen rechtswidrige Datenverarbeitungen zu Wehr zu setzen. Die Betroffenenrechte sind damit wesentliches Instrument der DSGVO. Auch beim IQTIG verarbeiten wir personenbezogene Daten, u. a. von Dienstleistern, Beschäftigten und Bewerbern. Daher sind auch wir im Rahmen unseres Datenschutz-Managements dazu verpflichtet, geeignete Prozesse zur Wahrnehmung der Betroffenenrechte zu schaffen. Kommt das IQTIG als verantwortliche Stelle einem Antrag der betroffenen Person nicht nach, können ein datenschutzaufsichtsrechtliches Verfahren sowie ein Bußgeld drohen.

2 Ziel der Richtlinie

Ziel der Richtlinie ist, durch definierte Prozesse und Zuständigkeiten eine fristgerechte, transparente und korrekte Bearbeitung von Anfragen betroffener Personen zu den ihnen nach der DSGVO zustehenden Betroffenenrechten zu gewährleisten.

3 Begriffsbestimmungen

In dieser Richtlinie werden folgende Begrifflichkeiten verwendet:

- **Personenbezogene Daten:** Personenbezogene Daten im Sinne dieser Richtlinie sind Angaben über eine identifizierte oder identifizierbare natürliche Person (z. B. Name, E-Mail-Adresse, Alter, Wohnort etc.). Daten, die ausschließlich Informationen über juristische Personen beinhalten, sind keine personenbezogenen Daten. Der Personenbezug entfällt ebenfalls bei einer vollständigen Anonymisierung, nicht aber bereits bei der Verwendung von Pseudonymen.

- **Betroffene:** Betroffene sind Personen, deren personenbezogene Daten beim IQTIG verarbeitet werden. Diese können sein: Mitarbeiter, Bewerber, Interessenten, Dienstleister etc.
- **Betroffenenrechte:** Betroffenenrechte sind die Rechte, die den betroffenen Personen nach der Datenschutz-Grundverordnung zustehen und zu deren Befolgung das IQTIG nach den Art. 12 ff. DSGVO verpflichtet ist.
- **Datenschutzanfragen bzw. Anfragen:** Jegliche Kontaktaufnahmen Betroffener in Hinblick auf die Ausübung und Geltendmachung der Betroffenenrechte, unabhängig von ihrer Form (mündlich, schriftlich oder per Mail) und Inhalt.

4 Betroffenenrechte

Den Betroffenen stehen nach der DSGVO folgende Betroffenenrechte zu, die dem IQTIG bekannt sind:

- Recht auf Auskunft (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Recht auf Widerspruch (Art. 21 DSGVO)
- Recht, nicht einer automatisierten Entscheidung unterworfen zu sein (Art. 22 Abs. 3 DSGVO)
- Recht auf Widerruf einer erteilten Einwilligung (7 Abs.3 DSGVO)

5 Grundsätze bei der Bearbeitung von Betroffenenrechten

Dem IQTIG ist bewusst, dass die Betroffenen insbesondere auch das Recht auf eine zeitnahe, vollständige und richtige, sowie transparente und unkomplizierte Bearbeitung Ihrer Betroffenenrechte haben (vgl. Art. 12 DSGVO). Daher erfolgt die Beantwortung der Anfragen stets in einer **präzisen, transparenten, verständlichen und leicht zugänglichen Form sowie in einer klaren und einfachen Sprache**. Beim IQTIG gelten daher bei der Wahrnehmung der Betroffenenrechte folgende Grundsätze:

5.1 Jede Anfrage wird beantwortet

Jede Person hat das Recht, die unter Punkt 4 der Richtlinie dargestellten Rechte geltend zu machen. Daher wird jede Anfrage ernst genommen. Da Datenschutzverlangen nicht immer eindeutig formuliert sind, ist jede eingehende Anfrage genau zu prüfen. Auch eine vermeintliche Kundenbeschwerde kann im Einzelfall als Auskunftsverlangen oder Löschverlangen auszulegen

sein. Umgekehrt stellt nicht jedes Auskunftersuchen ein Auskunftsverlangen im datenschutzrechtlichen Sinne dar. Bei Unklarheiten ist der Antragssteller vorsorglich zur Klarstellung seines Begehrens noch einmal zu kontaktieren.

Wir sind dazu verpflichtet, jede Anfrage zu beantworten. Auch wenn beim IQTIG keine personenbezogenen Daten zu dem Betroffenen vorhanden sind, muss dies der betroffenen Person mitgeteilt werden. In diesen Fällen wird eine so genannte **Negativauskunft** erteilt, d. h. die betroffene Person wird darüber informiert, dass keine personenbezogenen Daten zu ihr gespeichert sind.

5.2 Anfragen werden zeitnah beantwortet

Datenschutzanfragen von betroffenen Personen müssen **unverzüglich**, in jedem Fall **innerhalb eines Monats** bearbeitet werden (Art. 12 Abs. 3 DSGVO). Beim IQTIG werden Anfragen grundsätzlich innerhalb von zwei Wochen nach Eingang bearbeitet.

Im Ausnahmefall ist eine Fristverlängerung um weitere zwei Monate möglich, wenn dies

- aufgrund der Komplexität oder der Anzahl der Anträge erforderlich ist, und
- die betroffenen Personen innerhalb eines Monats über die Fristverlängerung und die Gründe für die Verzögerung unterrichtet wird.

5.3 Anfragen werden transparent und in einfacher Sprache beantwortet

Die Beantwortung des Auskunftsrechts muss in klarer und einfacher Sprache erfolgen. Der Datensatz muss so strukturiert sein, dass der Betroffene die einzelnen Kategorien (Verarbeitungszweck, verarbeitete Daten, Übermittlungen usw.) erkennen kann.

5.4 Anfragen werden unentgeltlich bearbeitet

Die DSGVO fordert vom IQTIG eine einfache und unkomplizierte Umsetzung der Betroffenenrechte. Die Bearbeitung und Beauskunftung der unter Nr. 3 dargestellten Betroffenenrechte erfolgt in der Regel entgeltfrei.

Ausnahmsweise kann ein Entgelt in angemessener Höhe verlangt werden, wenn die Anfrage offenkundig unbegründet oder missbräuchlich gestellt ist. Die Veranschlagung eines Entgeltes ist die Ausnahme. Sie ist stets einzelfallbezogen mit den Datenschutzbeauftragten abzustimmen. Die Gründe für die Veranschlagung eines Entgeltes sind zu dokumentieren.

5.5 Grundsatz der Richtigkeit und Wahrung Rechte Dritter

Anfragen Betroffener müssen richtig beantwortet werden und dürfen für das IQTIG nicht zu einem Datenschutzverstoß führen. Insbesondere muss darauf geachtet werden, dass Informationen nur an berechnigte Adressaten erteilt werden. Zu diesem Zwecke erfolgt vor bei jeder Anfrage eine Identitätsprüfung (Siehe auch Nr. 6.2). Außerdem werden in der Regel nur schriftlich beantwortet. Ausnahmen sind besonders zu begründen und mit dem Datenschutzbeauftragten abzustimmen.

Bei der Beantwortung von Anfragen dürfen keine Rechte dritter Personen beeinträchtigt werden. Davon umfasst sind z. B. Geschäftsgeheimnisse, Urheberrechte oder personenbezogene Daten anderer Personen. Sind solche Rechte Dritter betroffen, ist die Auskunft entsprechend zu beschränken. Hierfür kann beispielsweise eine Schwärzung derjenigen Informationen genügen, die bei einer Auskunftserteilung Rechte anderer Personen beeinträchtigen würden.

5.6 Ausnahmen bei missbräuchlichem Handeln

Wenn der Verdacht besteht, dass der Betroffene missbräuchlich handelt, kann neben den Regelungen aus Nr. 5.4 auch von einer Beauskunftung abgesehen werden. Missbräuchliches Handeln kann vorliegen, wenn ein Datenschutzverlangen schikanös, mit Schädigungsabsicht und in einer das IQTIG belastenden Weise vorgetragen wird. Ob tatsächlich ein missbräuchliches Handeln vorliegt, ist stets am Einzelfall und in Abstimmung mit dem Datenschutzbeauftragten zu prüfen. Das Absehen von der gewünschten Datenschutzanfrage wegen Missbrauchs ist zu begründen und zu dokumentieren.

Wird wegen Missbrauchs von der weiteren Bearbeitung abgesehen, muss die betroffene Person dennoch, **ohne Verzögerung, spätestens aber innerhalb eines Monats** nach Eingang des Antrags über die Gründe informiert haben. Darüber hinaus erfolgt eine Unterrichtung über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder bei Gericht ein entsprechender Rechtsbehelf einzulegen.

6 Zuständigkeiten bei der Beantwortung von Anfragen

Für die Bearbeitung der Betroffenenrechte ist zunächst jede Abteilung zuständig, die in ihren Verantwortungsbereich personenbezogene Daten der betroffenen Personen verarbeitet. Für die Beantwortung von Mitarbeiteranfragen und Bewerberanfragen ist grundsätzlich die Personalabteilung zuständig. Anfragen von Beteiligten der Qualitätssicherungsverfahren werden vom Verfahrenssupport bearbeitet. Sind personenbezogene Daten in Systemen mehrerer Abteilungen vorhanden, sorgt die zuständige Abteilung für die Koordinierung und vollständige Bearbeitung der Datenschutzanfrage. Anfragen, die an die allgemeine Datenschutzadresse eingehen, werden an die zuständige Abteilung weitergeleitet. Im Zweifel kann der Datenschutzbeauftragte einbezogen werden.

7 Praktische Umsetzung (Überblick)

7.1 Wesentliche Schritte bei Datenschutzanfragen Betroffener

Nach Eingang einer Datenschutzanfrage (Auskunftsbegehren, Antrag auf Löschung oder Berichtigung eines Betroffenen), erfolgt die Bearbeitung durch die zuständige Abteilung in folgenden Schritten:

1. Datenschutzanfragen werden nach Art und Umfang der Anfrage überprüft. Dabei ist stets der tatsächliche Wille des Antragstellers zu beachten. Die konkrete Bezeichnung in der Anfrage kann ein Indiz sein, ist jedoch nicht für sich alleine aussagekräftig. Bei Abgrenzungsfragen, umfangreichen und komplizierten Anfragen oder bei Verdacht auf Missbrauch wird der Datenschutzbeauftragte einbezogen.
2. Die Anfrage wird mit Eingangsdatum im Datenschutz-Management-System (verinice), dokumentiert (z. B. Ticketsystem mit Möglichkeit zur Feststellung des Bearbeitungsstandes/Fortschrittsverfolgung und zur Bewertung bzw. Überprüfung des Prozessablaufs).
3. Unverzögliche Mitteilung an den Antragssteller, dass sein Verlangen eingegangen ist und zeitnah bearbeitet wird
4. Prüfung der Identität des Antragstellers (s. Identitätsprüfung).
5. Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet wurden und ggf. Ermittlung aller relevanten Informationen für Beantwortung der Anfrage.
6. Beantwortung der Anfrage unter Beachtung der unter Punkt 5 der Richtlinie aufgestellten Grundsätzen.
7. Dokumentation der Antwort. Geht die Datenschutzanfrage mit einem (begründeten) Anspruch auf Datenlöschung einher, sind grundsätzlich alle Daten zu der betroffenen Person aus den Systemen zu löschen. Aus Nachweisgründen ist die Anfrage des Betroffenen für drei weitere Jahre beim Datenschutzbeauftragten aufzubewahren.

7.2 Identitätsprüfung

Es ist stets sicherzustellen, dass der Antragssteller auch wirklich der Betroffene ist. Deshalb muss vor Beantwortung der Anfrage die Identität des Antragstellers überprüft werden. Dabei müssen die Maßnahmen zur Überprüfung getroffen werden, die nach der Art der Kontaktanfrage angemessen sind. Es gelten daher folgende Grundsätze:

1. Erfolgt die **Anfrage auf dem Postweg**, genügt der Vergleich zwischen der aus früherer Kommunikation bekannten Postanschrift und der für die Anfrage verwendeten Postanschrift.
2. Bei **Anfragen per E-Mail** ist die bei der Anfrage verwendete E-Mail-Adresse mit der im IQTIG hinterlegten E-Mail-Adresse abzugleichen (z. B. Teilnehmerverwaltung). Liegt eine Übereinstimmung vor, so kann die Auskunft an die verwendete E-Mail-Adresse erfolgen.
3. Erfolgt eine **Anfrage per Telefon**, so darf die Auskunft nicht telefonisch erfolgen, da keine ausreichenden Maßnahmen zur Identitätsfeststellung getroffen werden können. Name und Anschrift des Anfragenden sind aufzunehmen und ist die Auskunft nach Abgleich der Daten und Übereinstimmung mit den hinterlegten Daten postalisch an die hinterlegte Adresse zu erteilen.

Weicht die Anschrift oder die E-Mail-Adresse des Anfragenden von den in der Datenbank hinterlegten Daten zum Anfragenden ab, so muss die Identität des Anfragenden auf anderen Weg festgesellt werden.

Dies kann beispielsweise durch Vorlage eines Ausweisdokuments vor Ort oder per Einsendung einer Kopie erfolgen. Der Betroffene ist darauf hinzuweisen, dass er alle Daten des Ausweisdokuments mit Ausnahme von Vor und Nachname, Anschrift, Geburtsdatum und Lichtbild schwärzen kann.

Möchte der Anfragende dem nicht nachkommen, kann die Auskunft lediglich postalisch an die im System hinterlegte Adresse erfolgen.

7.3 Vertraulichkeit der Anfrage

Das Antwortschreiben auf Datenschutzanfragen kann sensible Informationen enthalten und ist daher vertraulich zu behandeln. Antwortschreiben mit personenbezogenen Daten sollten daher grundsätzlich auf dem Postweg übermittelt werden. Werden die Antwortschreiben per E-Mail versendet, ist der Inhalt vorher zu verschlüsseln. Von einer Verschlüsselung sollte nur dann abgesehen werden, wenn die betroffene Person über das Sicherheitsrisiko informiert ist und sich ausdrücklich mit dem unverschlüsselten Versand der Informationen einverstanden erklärt hat. Bei einer Negativauskunft, oder bei der schlichten Bestätigung eines Löschbegehrens, kann von der Verschlüsselung ebenfalls abgesehen werden.

8 Informationen, Schulungen, Ansprechpartner

Diese Richtlinie steht allen Mitarbeitern im Intranet zum Abruf zur Verfügung. Mitarbeiter, die keinen Zugriff auf das Intranet haben, wird diese schriftlich zur Verfügung gestellt.

Alle Beschäftigten werden regelmäßig zum Datenschutz und insbesondere zum Umgang mit Betroffenenrechten geschult.

Bei Fragen, Anmerkungen etc. zu den Regelungen dieser Richtlinie wenden Sie sich bitte an folgenden Ansprechpartner:

- Datenschutzbeauftragter: Martin Schüller - datenschutz@iqtig.org

9 Aktualisierung der Richtlinie

Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.



Institut für Qualitätssicherung und
Transparenz im Gesundheitswesen

Löschkonzept

Umsetzung der DSGVO im IQTIG

- Anlage 7 zum Datenschutzkonzept des IQTIG -

Stand: 27. September 2018

Impressum

Thema:

Löschkonzept

Ansprechpartnerin/Ansprechpartner:

Gesine Schäfer-Reimers

Martin Schüller

Herausgeber:

IQTIG – Institut für Qualitätssicherung
und Transparenz im Gesundheitswesen

Katharina-Heinroth-Ufer 1

10787 Berlin

Telefon: (030) 58 58 26-0

Telefax: (030) 58 58 26-999

info@iqtig.org

<https://www.iqtig.org>

Inhaltsverzeichnis

Tabellenverzeichnis.....	5
Abbildungsverzeichnis.....	6
Abkürzungsverzeichnis.....	7
1 Einleitung und Hintergrund.....	8
1.1 Für das IQTIG relevante gesetzliche Normen	8
1.1.1 Allgemeine steuerrechtliche, haushaltsrechtliche und sozialversicherungsrechtliche Normen	8
1.1.2 Europäische Datenschutzgrundverordnung	8
1.1.3 Sozialgesetzbuch V	8
1.1.4 Weitere Normen	9
1.2 Definitionen.....	9
2 Analyse der Daten im IQTIG	11
2.1 Lokalisierung personenbezogener Daten im IQTIG	11
2.1.1 Daten in der IT-Abteilung	13
2.1.2 Daten in der Abteilung Verfahrensmanagement	22
2.1.3 Daten in der Abteilung Verfahrensentwicklung.....	23
2.1.4 Daten in der Abteilung Verfahrensgrundlagen	24
2.1.5 Daten in den Stabsbereichen	24
2.1.6 Daten in der Abteilung Kaufmännische Geschäftsführung.....	26
2.2 Kategorisierung der Daten	27
2.3 Definition der Löschregeln für die einzelnen Kategorien	28
2.4 Definition der Startzeitpunkte des Löschens	29
2.5 Definition der Löschklassen	29
2.6 Archivierung	30
2.7 Durchführung der Löschung.....	30
2.8 Dokumentation	31
3 Sonderfälle	32
3.1 Löschung auf Verlangen.....	32
3.2 Vorgaben des IQTIG an Unternehmen, die im Auftrag Daten verarbeiten	32
3.3 Umgang mit fehlerhaften Datenlieferungen	32

3.3.1	Im Rahmen des Aufbaus und der Erprobung von QS-Verfahren	32
3.3.2	Im Regelbetrieb	33
4	Einführungsvorgehen	34
4.1	Planung.....	34
4.2	Implementierung	34
4.3	Test.....	34
4.4	Fortschreibung	35

Tabellenverzeichnis

Tabelle 1: Charakterisierung der Eingangsdaten im IQTIG	13
Tabelle 2: Charakterisierung der Daten in der Teilnehmerverwaltung	14
Tabelle 3: Charakterisierung der Daten in der Kommunikationsplattform	15
Tabelle 4: Charakterisierung der Daten im Strukturierten Dialog	16
Tabelle 5: Charakterisierung der Daten auf den Websites des IQTIG	17
Tabelle 6: Charakterisierung der Daten der Auswertungen des IQTIG.....	20
Tabelle 7: Charakterisierung der Daten der IT-Systemadministration des IQTIG.....	21
Tabelle 8: Charakterisierung der Daten des Verfahrensmanagements.....	22
Tabelle 9: Charakterisierung der Daten der Verfahrensentwicklung	23
Tabelle 10: Charakterisierung der Daten der Verfahrensgrundlagen.....	24
Tabelle 11: Charakterisierung der Daten des Stabsbereichs Presse	25
Tabelle 12: Charakterisierung der Daten des Stabsbereichs Patientenbelange.....	25
Tabelle 13: Charakterisierung der Gremienverwaltung im IQTIG.....	26
Tabelle 14: Charakterisierung der Daten im Zeiterfassungs- und Projektmanagementsystem .	27
Tabelle 15: Matrix der Löschklassen	29

Abbildungsverzeichnis

Abbildung 1: Lokalisierung personenbezogener Daten im IQTIG	12
Abbildung 2: Löschprotokoll	30

Abkürzungsverzeichnis

Abkürzung	Bedeutung
BDSG	Bundesdatenschutzgesetz
bKpbD	Besondere Kategorien personenbezogener Daten
DSGVO	Kurztitel der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
EJ	Erfassungsjahr
G-BA	Gemeinsamer Bundesausschuss
IQTIG	Institut für Qualitätssicherung und Transparenz im Gesundheitswesen
pbD	Personenbezogene Daten
Qesü-RL	Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung
QS	Qualitätssicherung
QSKH-RL	Richtlinie über Maßnahmen der Qualitätssicherung in Krankenhäusern

1 Einleitung und Hintergrund

Im Rahmen seines Datenschutzkonzeptes ist das IQTIG verpflichtet, ein Konzept zur Löschung der bei ihm verarbeiteten Daten zu erstellen, um Speicherfristen einzuhalten und zu dokumentieren. Unter Beachtung von gesetzlichen und untergesetzlichen Aufbewahrungsfristen werden personenbezogene Daten nach Zweckfortfall gelöscht.

Dabei konkurrieren die Vorgaben der DSGVO zur Löschung von Daten mit anderen Regelungen, die die Aufbewahrung und Speicherung von Daten ausdrücklich verlangen. Beispielsweise schreiben steuerrechtliche Bestimmungen dem IQTIG die Aufbewahrung von Unterlagen vor. Zudem sehen auch Richtlinien des G-BA die Speicherung von Daten vor, insbesondere um Langzeitbetrachtungen und Follow-up Betrachtungen durchführen zu können. Andererseits sollen zum Zweck der sog. „sekundären Datennutzung“ die Daten aus den Qualitätssicherungsverfahren (QS-Verfahren) weiter durch das IQTIG vorgehalten werden.

Daher wird in diesem Konzept dargestellt, welche personenbezogenen Daten das IQTIG besitzt, regelmäßig erhebt, unregelmäßig erhält und wie es mit diesen oder Teilen davon umgeht sowie eine ggf. durchgeführte Löschung dokumentiert.

Für die Erstellung des Konzeptes hat sich das IQTIG an der DIN Norm 66398:2016:05 „Leitlinie zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten“ orientiert.

1.1 Für das IQTIG relevante gesetzliche Normen

1.1.1 Allgemeine steuerrechtliche, haushaltsrechtliche und sozialversicherungsrechtliche Normen

Es gelten die Sozialversicherungshaushaltsverordnung (SVHV), die Abgabenordnung (AO), die Verjährungsfristen des Bürgerlichen Gesetzbuchs (BGB) sowie weitere haushalts- und sozialrechtliche Regelungen.

1.1.2 Europäische Datenschutzgrundverordnung

Die DSGVO sieht in Artikel 5 vor, dass personenbezogene Daten für legitime Zwecke erhoben werden müssen und nur in damit vereinbar Weise weiterverarbeitet werden dürfen. Die Identifizierung der betroffenen Personen darf nur so lange möglich sein, wie es für die Zwecke, für die sie verarbeitet werden dürfen, erforderlich ist. Weiter erteilt die DSGVO den Betroffenen ein „Recht auf Vergessenwerden“ (Art. 17 DSGVO), die Möglichkeit eine erteilte Einverständnis zu widerrufen und gegen eine weitere Verarbeitung von Daten zu widersprechen.

1.1.3 Sozialgesetzbuch V

Das SGB V regelt in den §§ 136 ff. verpflichtende Aktivitäten für die Leistungserbringer, um an der Qualitätssicherung der medizinischen Versorgung mitzuwirken. Diese Maßnahmen werden

dann durch den Gemeinsamen Bundesausschuss (G-BA) in Richtlinien ausgestaltet. Hierbei werden personenbezogene Daten erhoben. § 299 SGB V regelt den Umgang mit den zu Zwecken der Qualitätssicherung erhobenen Daten.

Die für das IQTIG relevanten Richtlinien sind u. a.:

- QSKH-RL (Richtlinie über Maßnahmen der Qualitätssicherung in Krankenhäusern)
- Qesü-RL (Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung)
- DeQS-RL (Richtlinie zur datengestützten einrichtungsübergreifenden Qualitätssicherung)
- QSD-RL (Qualitätssicherungs-Richtlinie Dialyse)
- QFR-RL (Qualitätssicherungs-Richtlinie Früh- und Reifgeborene)
- oKFE-RL (Richtlinie für organisierte Krebsfrüherkennungsprogramme)

Weiterhin ist in § 137a Abs. 10 SGB V geregelt, dass der G-BA das IQTIG mit der Auswertung der für die Qualitätssicherung erhobenen Daten für Zwecke der wissenschaftlichen Forschung und der Weiterentwicklung der Qualitätssicherung beauftragen kann, die sog. „sekundären Datennutzung“. Dies steht jedoch im Widerspruch zu den Löschvorgaben aus den Richtlinien des G-BA, die bestimmen, dass QS-Daten aus abgeschlossenen QS-Verfahren zu löschen sind. Sofern die Regelungen des G-BA die Löschung der QS-Daten vorgeben, wird das IQTIG die personenidentifizierenden Bestandteile der QS-Daten nach vorheriger Rücksprache mit dem G-BA anonymisieren.

1.1.4 Weitere Normen

Für ausgewählte Daten zählen weitere Normen wie z. B. das Europäische Vergaberecht, das nationale Vergaberecht, arbeitsrechtliche Regelungen u. a..

Daher ist die Liste der Normen nicht vollständig und wird mit der Fortschreibung des Löschkonzepts ggf. fortgeführt.

1.2 Definitionen

Personenbezogene Daten (pbD)

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO).

Besondere Kategorien personenbezogener Daten (bKpbD)

Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person sind besonders zu schützen und dürfen nur mit besonderer gesetzlicher Ermächtigung oder mit Einwilligung der betroffenen Person verarbeitet werden (Art. 9 Abs. 1 DSGVO).

2 Analyse der Daten im IQTIG

Folgende Grundsätze gelten im IQTIG bezüglich der Speicherung von Daten:

- Vor der Vervielfältigung von Dateien soll genau überlegt werden, ob dieser Schritt notwendig ist. Dies verhindert das mehrfache Ablegen von Daten und Dokumenten an vielen Orten und somit deren Löschung und begrenzt die Datenmenge, die auf den Servern des IQTIG gespeichert, gesichert und ggf. wiederhergestellt werden muss.
- Alle Systeme, auf denen Daten gespeichert sind (Dateisystem, Datenbanken, SFTP-Server), verfügen über ein System zum Schutz vor unberechtigten Zugriffen, ein Berechtigungssystem. Alle Zugriffe und Zugriffsversuche werden protokolliert.
- Daten dürfen ausschließlich in gesicherten Verzeichnissen oder Datenbanken abgelegt werden.
- Alle Benutzeraccounts im IQTIG sind an Personen gebunden, so dass Zugriffe entsprechend zurückverfolgt werden können.

2.1 Lokalisierung personenbezogener Daten im IQTIG

Für jede Abteilung des Instituts wird geprüft, welche personenbezogenen Daten dort gespeichert und verarbeitet werden. Ausgehend von diesem organisatorischen Anknüpfungspunkt wurde geprüft, wo diese Daten gespeichert sind.

Dabei wurden erfasst:

- die Datenkategorien, d. h. die Art der Daten;
- welche davon zu besonderen Kategorien personenbezogener Daten gehören;
- die Dauer ihrer Nutzung;
- ob und wie lange die betreffenden Daten aufbewahrungspflichtig sind;
- auf welchem System oder Datenträger diese Daten gespeichert werden;
- welche Datenzu- und abflüsse in bzw. von anderen Systemen es gibt, die ebenfalls berücksichtigt werden müssen.

Ausgangspunkt für die Lokalisierung der Daten waren die verarbeitenden Applikationen, welche im IQTIG im Einsatz sind, hier zunächst die selbstentwickelte Software. Hinzu kommen Daten aus der Verwaltung (Personal, Bewerber, Lieferanten, Ansprechpartner für Gremien/Veranstaltungen).

2.1.1 Daten in der IT-Abteilung

2.1.1.1 Software zur Pseudonymisierung von Eingangsdatensätzen

Das IQTIG erhält im Rahmen der externen Qualitätssicherung nach den §§ 136 ff. SGB V eine Vielzahl von Daten, von denen einige Personenbezug aufweisen. Daher werden alle Eingangsdaten mit einem Patientenpseudonym vor jeder weiteren Verarbeitung im IQTIG einer Prozedur unterzogen, in der aus den gelieferten Patientenpseudonyme per Randomisierung neue Pseudonyme generiert, die später als Anonyme verwandt werden können. Die Zuordnung von gelieferten Patientenpseudonym und neuem Pseudonym erfolgt mittels einer Mappingtabelle. Eine eindeutige Vorschrift zur Erstellung des Pseudonyms führt dazu, dass z. B. aus zwei einzelnen Datenlieferungen ein Follow-up Datensatz identifiziert werden kann.

Die Datensätze liegen im weiteren Prozess nur noch pseudonymisiert bzw. anonymisiert vor. Eine Anonymisierung der Daten erfolgt dadurch, dass die Mapping-Tabelle nach Ablauf der Löschrfrist gelöscht wird.

Tabelle 1: Charakterisierung der Eingangsdaten im IQTIG

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
QSKH-Daten	Daten, die durch die QSKH gefordert werden ohne Patientenpseudonyme	Bis zur Weiterverarbeitung	QSKH-RL	Bis zum Wegfall des Zwecks	E-Mail Server	Zufluss: E-Mail der Leistungserbringer Abfluss: weitere Verarbeitungsprozesse
Qesü-Daten	Daten mit Patientenpseudonymen	Bis zur Weiterverarbeitung	Qesü-RL	Bis zum Wegfall des Zwecks	SFTP-Server	Zufluss: Lieferungen der Vertrauensstelle Abfluss Pseudonymisierungsprogramm
Pseudonymwechsel-Mappingtabelle	Einander zugeordnete Pseudonyme mit Personenbezug (inkl. bKpbD)	Bis die Änderung der Pseudonyme abgeschlossen ist		Bis die Änderung der Pseudonyme abgeschlossen ist, danach wird die Tabelle gelöscht	Dateisystem	Zufluss: Datenentgegennahme Abfluss: weitere Verarbeitungsprozesse

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Ersatzpseudonym-Mappingtabelle	Einander zugeordnete Pseudonyme mit Personenbezug	Bis zum Entfall des Zwecks			Dateisystem	Zufluss: Datenentgegennahme Abfluss: weitere Verarbeitungsprozesse
Rohdatenpool	Spezifikationskonforme Datensätze in verschiedenen Versionen				Datenbank	
Importdatenpool	Datensätze in nur einer Version				Datenbank	
Snapshotdatenpools	Datensätze für eine konkrete Auswertung				Datenbank	
Mapped Datenpools	Datensätze mehrerer Verfahrensjahre für eine konkrete Auswertung				Datenbank	
Auswertungsdatenpools	Datensätze für eine konkrete Auswertung				Datenbank	

2.1.1.2 Daten in der Teilnehmerverwaltung

Die Teilnehmerverwaltung beinhaltet an zentraler Stelle alle Teilnehmer, die im IQTIG an der Entwicklung oder Durchführung der Qualitätssicherung beteiligt sind, und stellt hierfür ein Stammdatensystem dar. Alle Personen, die sich an der Website oder den Portalen des IQTIG anmelden wollen, um z. B. Daten zu liefern, Berichte abzurufen, am Strukturierten Dialog teilzunehmen oder auch Mitglieder von Bundesfachgruppen werden in der Teilnehmerverwaltung angelegt.

Tabelle 2: Charakterisierung der Daten in der Teilnehmerverwaltung

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Teilnehmerdaten	Strukturierte Daten in einer relationalen Datenbank (keine bKpD)	Bis zum Widerruf der Einwilligung			Datenbank	Zufluss: Einrichtung der Verfahrensteilnehmer durch Selbst- oder Fremdgistrierung Abfluss: keiner

Die Teilnehmerverwaltung beinhaltet Daten mit Personenbezug (Name, Kontaktdaten u. ä.), aber keine besonderen Kategorien personenbezogener Daten.

2.1.1.3 Daten in der Kommunikationsplattform

Die Kommunikationsplattform ist ein Extranet des IQTIG und dient zum Austausch des Verfahrenssupports des IQTIG mit den Verfahrensteilnehmern bei Fragen zum gesamten Prozess. Hier werden Anfragen koordiniert abgearbeitet und Lösungen ggf. allen Verfahrensteilnehmern zur Verfügung gestellt. Bis zur Anbindung der Kommunikationsplattform an die zentralen Systeme des IQTIG wird diese eine eigenständige Teilnehmerverwaltung haben. Es werden dort keine besonderen Kategorien personenbezogener Daten verarbeitet.

Tabelle 3: Charakterisierung der Daten in der Kommunikationsplattform

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Teilnehmerdaten	Strukturierte Daten in einer relationalen Datenbank (keine bKpD)	Bis zum Widerruf der Einwilligung			Datenbank	Zufluss: Einrichtung der Verfahrensteilnehmer durch Selbst- oder Fremdgistrierung Abfluss: keiner
Daten zu Anfragen zum Verfahren	Inhalte der Anfragen im Fließtext ggf. mit Kürzeln zur Identifikation des	Bis zur Klärung der Anfrage und ggf. Dokumentationszwecken		Bis zum Entfall des Zwecks	Datenbank	Zufluss: E-Mail an den Verfahrenssupport Abfluss: Nachstellung von Fehlerfällen

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
	Leistungserbringers oder des Datensatzes, ggf. auch Binärdaten wie Screenshots von Fehlermeldungen oder PDF-Berichte					im Verarbeitungsprozess

Die Mitarbeiter im Verfahrenssupport und besonders im Datenmanagement sind besonders geschult in der Verarbeitung allgemeiner Daten und der Erkennung besonderer Kategorien personenbezogener Daten. Werden entgegen des Zwecks der Kommunikationsplattform dennoch bKpD übermittelt, werden Sie diese gemäß Kapitel 3.3 unverzüglich bearbeitet.

2.1.1.4 Daten im Strukturierten Dialog

Im Strukturierten Dialog treten die Leistungserbringer und das IQTIG in seiner Funktion als Bundesauswertungsstelle in Kontakt, um die im Rahmen der vergleichenden Qualitätssicherung auffällige Fälle zu besprechen. Dabei identifizieren sich die am System anmeldenden Personen mit der Kombination „Benutzername/Kennwort“, die in der Teilnehmerverwaltung hinterlegt ist.

Tabelle 4: Charakterisierung der Daten im Strukturierten Dialog

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Daten zur Diskussion eines konkreten Falls	Text, E-Mails, Scans, ggf. Auszüge der Patientenakte inkl. bKpD	Bis zum Abschluss des Strukturierten Dialogs	Bis zum Entfall des Zwecks		Datenbank	Zufluss: Durch Einstellung der BAS, durch Eintragung und Upload durch den Leistungserbringer Abfluss: Keiner

Die Mitarbeiter im Verfahrenssupport sind besonders geschult in der Verarbeitung personenbezogener Daten und der Erkennung besonderer Kategorien personenbezogener Daten. Werden

entgegen des Zwecks dennoch bKpD übermittelt, z. B. eine Stelle aus der Patientenakte zur Besprechung eines Falles, in der besondere Kategorien personenbezogener Daten nicht geschwärzt sind, so werden Sie diese gemäß Kapitel 3.3 unverzüglich bearbeitet.

2.1.1.5 Daten auf den Websites des IQTIG

Auf den verschiedenen Websites des IQTIG werden Daten erhoben, die wie folgt charakterisiert sind:

Tabelle 5: Charakterisierung der Daten auf den Websites des IQTIG

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Logfiles	Textbasierte Einträge die enthalten, welche Seiten und Daten wann von welcher IP abgerufen wurden	Zum Erkennen von Angriffen			Webserver	Zufluss: Automatisiert durch die externen Benutzer der Websites Abfluss: in Logverzeichnisse
Statistikinformationen	Textbasierte Informationen zum Verhalten der Nutzer der Websites, anonymisiert	Zum Erkennen des Nutzerverhaltens und zur Optimierung der Nutzung			Webserver, Statistikdienst Matamo	Zufluss: Automatisiert durch die externen Benutzer der Websites Abfluss: zu Matamo, ggf. in PDF-Format als Bericht ins Dateisystem
Fachliches Log in den Webanwendungen	Logging von definierten Benutzeraktionen in einer Website, mit Personenbezug	Zum Nachweis von Interaktionen im System	Bis zum Entfall des Zwecks		In der Website selbst	Zufluss: übt ein eingeloggter Benutzer in einer Website Aktionen aus, die als zu loggen definiert sind, dann wird diese

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
						Aktion protokolliert. Hiermit kann das IQTIG den Nachweis erbringen, wann und durch welchen Nutzer bspw. der Abruf eines Berichts erfolgt ist. Abfluss: Fachliches Log der Website
Login-Daten	Login-Token	Zum Nachweis von Interaktionen im System	Bis zum Entfall des Zwecks		Logfiles	Zufluss: Sofern eine Authentifizierung des Nutzers z.B. zum Download eines Berichts erforderlich ist, werden die Login-Daten mit der Teilnehmerverwaltung abgeglichen und bei erfolgreichem Login ein Token übermittelt, der nur für die Dauer der Sitzung einmalig gilt und keine personenbezogenen Daten enthält

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
						Abfluss: in die Logfiles

2.1.1.6 Daten in der Auswertung

Die QS-Daten, die anlass- und bedarfsbezogenen Auswertungen unterzogen werden, um vergleichende Betrachtungen zwischen den Leistungserbringern herzustellen, sind hinsichtlich des Patientenpseudonyms bereits nach der ersten Eingangsprüfung durch ein Ersatzpseudonym¹ pseudonymisiert.

Die QS-Daten stellen selbst aber Gesundheitsdaten dar, die als besondere Kategorien personenbezogener Daten gelten und besonders zu schützen sind. Für Langzeitbetrachtungen ist die Verknüpfung von Datensätzen über die Patientenpseudonyme/Ersatzpseudonyme bzw. Anonyme für die Erfüllung der Aufgaben des IQTIG zwingend erforderlich.

Der Zweck der Verarbeitung der Daten ergibt sich aus dem QS-Verfahren, das durch eine Richtlinie des G-BA geregelt wird. Mit der Beendigung eines QS-Verfahrens (z. B. nach Ablauf eines Follow-up Zeitraums sowie nach Auswertung und Bewertung) wären die betroffenen Daten grundsätzlich zu löschen, es sei denn, andere Zwecke erlauben die weitere Verarbeitung, z. B. zu Zwecken der sekundäre Datennutzung. Aus diesem Grund werden die QS-Daten nach Beendigung eines QS-Verfahrens oder eines Follow-up Zeitraums nicht gelöscht, sondern für die QS-Auswertung gesperrt und nur noch für die sekundäre Datennutzung vorgehalten und ggf. anonymisiert.

Da nach den Regelungen der sekundären Datennutzung nicht die Daten, sondern die Auswertungsergebnisse zu anonymisieren sind (vgl. § 137a Abs. 10 Satz 3 und 4 SGB V i. V. m. 8. Kapitel § 4 VerfO G-BA), sind Inhalt und Art späterer Auswertungen nicht eingeschränkt, so dass eine vorgreifende Anonymisierung der QS-Daten ggf. dazu führen würde, dass eine mögliche Zusammenführung von QS-Daten für eine später vorzunehmende Auswertung nicht mehr vorgenommen werden kann.

Daher wird das IQTIG die entsprechenden Datenfelder (z. B. Geschlecht, Alter) nicht löschen, so lange die Verpflichtung besteht, noch nicht näher spezifizierte Auswertungen zur Beantwortung von Anträgen aus der sekundären Datennutzung zu erstellen. Jedoch wird das IQTIG die betreffenden Daten insoweit sperren, dass sie nur noch befugten Personen im Rahmen der sekundären Datennutzung eingesehen und verarbeitet werden können.

Angesichts der besonderen Natur der Daten wird das IQTIG sorgfältig sicherstellen, dass Auswertungsergebnisse aus dem Verfahren der sekundären Datennutzung nur in anonymisierter Form an den Antragssteller übermittelt werden. Es führt die Anonymisierung der Auswertungen auf Grundlage eines eigenen Konzepts nach dem aktuellen Stand der Technik (BSI) durch. Das

¹ s. Konzept des IQTIG zur Handhabung von Patientenpseudonymen vom April 2018

Anonymisierungsverfahren stellt sicher, dass eine Reidentifizierung natürlicher Personen oder Leistungserbringer auch unter Zusatzwissen des Antragsstellers sicher ausgeschlossen ist. Die Anonymisierung der Auswertungsergebnisse wird durch den Datenschutzbeauftragten des IQTIG auf ihre Datenschutzkonformität hin geprüft².

Tabelle 6: Charakterisierung der Daten der Auswertungen des IQTIG

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Statistische Auswertungen	Numerische und textbasierte Daten, Formeln, Indikatoren, Binärdateien wie generierte Diagramme und statistische Auswertungen		Bis zum Entfall des Zwecks		Dateisystem	Zufluss: aus den Auswertungs- und Statistikprogrammen Abfluss: auf das Dateisystem, nach extern via SFTP

2.1.1.7 Altdaten vor der Gründung des IQTIG

Daten, die das IQTIG von den früheren Institutionen nach § 136 bzw. § 137a SGB V (a. F.) erhalten hat, wurden geprüft und bei der entsprechender Zweckbestimmung in die Infrastruktur des IQTIG übernommen.

Veraltete Datenträger oder Datensätze, für deren Verarbeitung keine Rechtsgrundlage besteht, wurden bzw. werden vernichtet (z. B. Datensätze aus QS-Dialyse eines früheren Datenanalytikers).

2.1.1.8 Daten in der IT-Systemadministration / Systemdaten

Die Mitarbeiter des IQTIG erzeugen bei der täglichen Arbeit gleichfalls Daten: Hier handelt es sich um Daten zum Nachweis ihrer Tätigkeiten, z. B. Daten in Log-Files zur Dokumentation, wann ein Mitarbeiter eine Datei bearbeitet oder gelöscht hat. Diese Daten werden wie folgt aufbewahrt bzw. gelöscht:

² Siehe Datenschutzkonzept des IQTIG, Kapitel 7.8 „Datenverarbeitung beim Verfahren der sekundären Datennutzung“ (Version 2.3 vom 13.09.2018)

Tabelle 7: Charakterisierung der Daten der IT-Systemadministration des IQTIG

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Anmelde- daten der Benutzer	Die Windows- Benutzer melden sich an der Do- mäne an und ab		Nachweis des ge- schäftlichen Handelns		Microsoft Serverbe- triebssys- tem	Zufluss: Aus Anmeldun- gen Abfluss: Ba- ckup
Anmelde- daten der Benutzer bei Operati- onen auf Dokumen- ten	Bearbeiten oder Lös- chen Be- nutzer Do- kumente auf dem Windows- Dateisys- tem, so werden diese Aktio- nen gespei- chert		Nachweis des ge- schäftlichen Handelns		Microsoft Serverbe- triebssys- tem	Zufluss: Aus Anmeldun- gen Abfluss: Ba- ckup
Postfächer der Benut- zer	Dienstliche E-Mail Kor- respondenz		Nachweis des ge- schäftlichen Handelns		E-Mail Ser- ver	Zufluss: Empfang und Senden von E-Mails Abfluss: Ba- ckup
Adresslis- ten und Ka- lender der Benutzer	Im E-Mail Client durch den Benutzer angelegte Adresslis- ten und Ka- lenderein- träge	Bis Ende der Bezie- hung	Komfort- Funktion		E-Mail Ser- ver	Zufluss: An- legen der Daten durch den Benutzer Abfluss: Ba- ckup

Durch die interne organisatorische Regelung, dass E-Mail Postfächer ausschließlich dienstliche genutzt werden dürfen, ist sichergestellt, dass sich im Postfach der Mitarbeiter keine privaten Daten befinden.

2.1.2 Daten in der Abteilung Verfahrensmanagement

Die Abteilung Verfahrensmanagement (Abt. VM) betreut die QS-Verfahren, die sich im „Regelbetrieb“ befinden. Sie organisiert darüber hinaus die Treffen der Bundesfachgruppen (BFG) sowie weiterer Beteiligter an der Durchführung der QS-Verfahren und führt Fachwissen für die Auswertung, die Durchführung und die Weiterentwicklung der Verfahren zusammen.

Tabelle 8: Charakterisierung der Daten des Verfahrensmanagements

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Kontaktdaten der Mitglieder der BFG	Strukturierte Daten wie Name, Vorname, E-Mail Adresse				Dateisystem, E-Mail Verteilerlisten	Zufluss: Durch manuelle Einrichtung und durch die Teilnehmerverwaltung Abfluss: durch manuelle Einrichtung
Kontaktdaten von Personen, die eine Anfrage an das VM stellen	Textbasierte Daten mit personenbezogenen Daten wie Absenderinformationen				E-Mail System	Zufluss: Durch die E-Mail Anfrage eines externen Interessenträgers Abfluss: keiner

Die Mitglieder der BFG und anderer Gremien sind in der Teilnehmerverwaltung gespeichert (s. o.). Die Mitglieder unterschreiben eine Erklärung vor der Teilnahme am QS-Verfahren, in welcher auch die Einwilligung für die Datennutzung erteilt wird. Es wird regelmäßig überprüft, ob die Einwilligungen erneuert oder erweitert werden müssen.

Da die Mitarbeiter der Abteilung Verfahrensmanagement als Ansprechpartner extern bekannt sind, werden Anfragen von Dritten direkt an die Mitarbeiter gesandt. Um eine Weiterverteilung der persönlichen Daten (Name, E-Mail-Adresse ...) der anfragenden Person zu vermeiden, sind die Mitarbeiter der Abt. VM verpflichtet, diese Daten nicht durch einfache Weiterleitung der E-Mail an große Verteilergruppen zu verbreiten und die Anfrage zunächst im kleinen Rahmen zu klären. Ist es notwendig, die anfragende Person ggf. in Adress- oder Verteilerlisten aufzunehmen, so wird eine entsprechende schriftliche Einwilligung eingeholt.

2.1.3 Daten in der Abteilung Verfahrensentwicklung

Die Abteilung Verfahrensentwicklung (Abt. VE) entwickelt im Auftrag des G-BA Konzeptskizzen, neue Verfahren und führt Machbarkeitsstudien durch. Der Fachbereich Befragungen in der Abt. VE konzipiert und erstellt dabei Befragungen von Einrichtungen und Patienten.

Ggf. werden auch hier personenbezogene Daten (u. U. auch bKpBD) erhoben, die wie die QS-Daten aus den regulären QS-Verfahren ebenfalls nach ihrer Verarbeitung gelöscht oder anonymisiert werden.

Tabelle 9: Charakterisierung der Daten der Verfahrensentwicklung

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Kontakt- daten von Ex- perten in Entwick- lungspro- jekten	Struktu- rierte Da- ten wie Name, Vor- name, E- Mail Ad- resse	Bis zum Entfall des Zwecks	Aus Auftrag des G-BA und Einwil- ligung		Dateisys- tem, E-Mail Verteilerlis- ten	Zufluss: Durch ma- nuelle Ein- richtung Abfluss: durch ma- nuelle Ein- richtung und manu- elle Weiter- gabe
Kontakt- daten von Personen in Befragungs- projekten	Struktu- rierte Da- ten wie Name, Vor- name, E- Mail Ad- resse	Bis zum Entfall des Zwecks	Aus Auftrag des G-BA und Einwil- ligung		Dateisys- tem, E-Mail Verteilerlis- ten	Zufluss: Durch ma- nuelle Ein- richtung Abfluss: durch ma- nuelle Ein- richtung, manuelle Weitergabe
Kontakt- daten von Personen, die initiativ das IQTIG anschrei- ben	Textba- sierte Da- ten mit per- sonenbezog- enen Daten wie Absen- derinfor- mationen	Noch kein Zweck vor- handen			E-Mail Sys- tem	Zufluss: Durch die E-Mail An- frage eines externen Interessen- trägers Abfluss: keiner

Da die Projekte der Verfahrensentwicklung zumeist völlig neue Projekte sind, werden die notwendigen Informationen und Experten aus öffentlich zugänglichen Quellen gewonnen. So werden Experten z. B. aufgrund ihrer wissenschaftlichen Publikationen oder durch sonstige Recherchen im Internet angesprochen.

Im Falle der Beteiligung als Experte wird die Einwilligung eingeholt, die Kontaktdaten für dieses Projekt zu nutzen. Hierfür wird das Formular zur Einwilligung in die Datennutzung mit einem entsprechend definierten Zweck genutzt und zu Dokumentationszwecken abgelegt. Nach Abschluss des Projekts, werden diese Kontaktdaten gelöscht - es sei denn, es liegt eine Einwilligung zur weiteren Speicherung für spätere Projekte vor.

Dies gilt auch für die Mitarbeiter des Fachbereichs Befragungen die bei der Erstellung von Fragebögen auf die Trennung von personenbezogenen und sonstigen QS-Daten achten, in dem z.B. Anschreiben und Fragebogen voneinander unabhängig gestaltet werden und der Fragebogen ggf. pseudonymisiert wird.

2.1.4 Daten in der Abteilung Verfahrensgrundlagen

Der Fachbereich Sozialdaten in der Abteilung Verfahrensgrundlagen verarbeitet QS-Daten (insb. Sozialdaten bei den Krankenkassen) im Rahmen der Entwicklung und Durchführung von QS-Verfahren.

Tabelle 10: Charakterisierung der Daten der Verfahrensgrundlagen

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Verfahrensspezifische Sozialdaten	Strukturierte pseudonymisiert Daten		Bis zum Entfall des Zwecks, ggf. nachweispflichtig		Dateisystem, Datenbanken, SFTP-Server	Zufluss: auf Anforderung von der VS Abfluss: in anonymisierte Auswertungen

Hinsichtlich dieser Daten ist durch die Pseudonymisierung an einer frühen Stelle im Verfahren sichergestellt, dass sich keine patientenidentifizierenden Daten in den zur Auswertung stehenden Daten befinden.

2.1.5 Daten in den Stabsbereichen

2.1.5.1 Daten im Stabsbereich Presse

Im Stabsbereich Presse liegen in erster Linie Pressekontakte und Presseanfragen vor. Werden externe Dienste genutzt, werden mögliche Löschbedingungen beachtet.

Darüber hinaus kommt es aber auch zu unmittelbaren Kontakten mit einzelnen Redakteuren, Vertretern juristischer Personen oder Privatpersonen.

Tabelle 11: Charakterisierung der Daten des Stabsbereichs Presse

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Pressekontakte	Strukturierte Daten mit Name, Adresse und E-Mail z.B. als Absenderinformationen		Bis zum Entfall des Zwecks, ggf. nachweispflichtig		E-Mail System, Kontaktliste auf Dateisystem	Zufluss: via E-Mail vom Anfragenden Abfluss: keiner

Die Mitarbeiter der Presseabteilung werden dahingehend geschult, dass Sie Kontaktdaten sorgfältig behandeln und nicht unsachgemäß weitergeben. Wird eine Anfrage z. B. an eine Fachabteilung weiter geleitet, wird diese womöglich um die personenbezogenen Daten bereinigt.

Verlangt ein Pressekontakt die Löschung, so setzt der Stabsbereich Presse dies um und veranlasst ggf. auch die Löschung duplizierter Daten, in dem er die betroffenen Abteilungen informiert.

2.1.5.2 Daten im Stabsbereich Patientenbelange

Im Stabsbereich Patientenbelange liegen Kontakte und Korrespondenz zu anfragenden Patienten.

Tabelle 12: Charakterisierung der Daten des Stabsbereichs Patientenbelange

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Patientenkontakte	Strukturierte Daten mit Name, Adresse und E-Mail z.B. als Absenderinformationen, ggf. bKpbD		Bis zum Entfall des Zwecks, ggf. nachweispflichtig		E-Mail System, Kontaktliste auf Dateisystem	Zufluss: via E-Mail vom Anfragenden Abfluss: keiner

Die Mitarbeiter im Stabsbereich Patientenbelange des IQTIG werden hinsichtlich des Datenschutzes gesondert geschult, da die Patientendaten sowohl personenbezogen sind und im Einzelfall auch besondere Kategorien personenbezogener Daten beinhalten. Sie werden dahingehend sensibilisiert, dass die Daten höchst vertraulich behandelt und nur unter Sorgfalt weitergeben und dupliziert werden. Wird eine Anfrage z. B. an eine Fachabteilung weiter geleitet, wird diese womöglich um die personenbezogenen Daten bereinigt.

Verlangt ein Patientenkontakt die Löschung, so setzt der Stabsbereich Patientenbelange dies um und veranlasst ggf. auch die Löschung duplizierter Daten, in dem er die betroffenen Abteilungen informiert.

2.1.5.3 Weitere Stabsbereiche: Recht, interne Qualitätssicherung

Auch hier gelten die allgemeinen Ausführungen hinsichtlich des Umgangs mit externen Kontakten.

2.1.6 Daten in der Abteilung Kaufmännische Geschäftsführung

2.1.6.1 Kontakte zu Gremien

Das IQTIG hat satzungsgemäße Gremien. Hierzu werden durch die Trägerorganisationen Teilnehmer benannt.

Tabelle 13: Charakterisierung der Gremienverwaltung im IQTIG

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Kontaktdaten der Gremienmitglieder	Strukturierte Daten wie Name, Vorname, E-Mail Adresse			Nach stiftungsrechtlichen Vorgaben	E-Mail System, Dateisystem	Zufluss: Durch manuelle Einrichtung Abfluss: manuell

2.1.6.2 Daten im Zeiterfassungs- und Projektmanagementsystem BCS

Im Zeiterfassungs- und Projektmanagementsystem BCS werden Anwesenheitszeiten sowie Urlaubs- und Krankheitszeiten erfasst und gespeichert. Die Projekte des IQTIG werden ebenfalls in BCS geplant und gesteuert.

Tabelle 14: Charakterisierung der Daten im Zeiterfassungs- und Projektmanagementsystem

Daten	Art der Daten	Dauer der Nutzung	Aufbewahrungspflicht	Dauer der Aufbewahrung	Speicherort	Datenzu- und abflüsse
Erfassung von Anwesenheitszeit	Beginn und Ende der täglichen Arbeitszeit sowie Pausen und Urlauben		Nach arbeits-, steuer- und sozialrechtlichen Vorgaben		BCS	Zufluss: Durch Erfassung des Mitarbeiters Abfluss: keiner
Erfassung von erbrachten Leistungen für Projekte	Dauer der Arbeitszeit und Beschreibung sowie Zuordnung zu einem Projekt				BCS	Zufluss: Durch Erfassung des Mitarbeiters Abfluss: statistische Auswertungen von Projekten
Krankheitstermine	Datum der Abwesenheit		Nach sozialrechtlichen Vorgaben		BCS	Zufluss: Durch Erfassung des Mitarbeiters Abfluss: keiner

Die Mitarbeiter der kaufmännischen Geschäftsführung sind sich der Sensibilität der Daten bewusst und werden hinsichtlich des Datenschutzes regelmäßig geschult. Die für den Austausch z. B. mit Versicherungen notwendigen Daten werden nicht häufiger als notwendig dupliziert und nur an zugriffsgeschützten Stellen aufbewahrt.

2.2 Kategorisierung der Daten

Die erhobenen Datenarten werden in Kategorien unterteilt, für welche eine gleiche Aufbewahrungsdauer definiert werden kann. Folgende Kategorien werden abgeleitet:

- QS-Daten ohne Personenbezug
- QS-Daten pseudonymisiert
- Weitere QS-Daten

- Fehlerhafte Eingangsdatensätze
- Eingangsdatensätze mit besonderem Analysebedarf
- Stammdaten und Vertraulichkeitserklärungen von Verfahrensteilnehmern
- Kernstammdaten des IQTIG (Urkunden, Zertifikate)
- Verträge
- Personaldaten
- Bewerberdaten
- Buchhaltungsdaten
- Aufzubewahrende Daten nach haushaltsrechtlichen Regelungen
- Sonstige aufzubewahrende Daten

Werden Daten zwar nicht mehr zu Ihrem ursprünglichen Zweck benötigt (etwa um einen Vertrag durchzuführen), müssen aber aufgrund gesetzlicher Aufbewahrungspflichten aufbewahrt werden, geht damit eine rechtlich zulässige Zweckänderung einher.

2.3 Definition der Löschregeln für die einzelnen Kategorien

Die DSGVO sieht vor, dass personenbezogene Daten nur solange gespeichert werden dürfen, wie dies für die Zwecke, für die sie erhoben wurden, erforderlich ist (Art. 5 Abs. 1 lit. e) DSGVO - Speicherbegrenzung). Daher sollte für jede Kategorie anhand von Erhebungsdatum, voraussichtlicher (durchschnittlicher) Bearbeitungszeit und dem Beginn der jeweiligen Aufbewahrungsfrist eine Löschregel bestimmt werden. Die Anzahl der Löschregeln soll dahingehend limitiert werden, dass es je Datenart nur genau eine Löschregel gibt.

Zur Reduzierung der Komplexität sollen die Löschfristen auf folgende Fristen vereinheitlicht werden:

- Daten, für deren Verarbeitung das IQTIG keine Ermächtigungsgrundlage hat, müssen **sofort** gelöscht werden. Dies kann z. B. vorkommen, wenn im Strukturierten Dialog ein Auszug aus einer Krankenakte hochgeladen wird und bKpD nicht geschwärzt worden sind.
- Für Daten, die nicht sofort gelöscht werden müssen, für die aber keine besondere Aufbewahrungspflicht besteht und die personenbezogene Daten enthalten können (z. B. Log-Files), wird die Löschfrist auf **zwei Monate** festgelegt.
- Für Daten, deren Verarbeitung mehr als drei Monate betragen kann, wird eine Löschfrist von **sechs Monaten** nach Abschluss der Verarbeitung definiert.
- Die regelmäßige Verjährungsfrist nach § 195 BGB beträgt drei Jahre. Da die Rechtsvorschriften die Verjährung mit der Jahresgrenze definieren, empfiehlt die DIN 66398 das Setzen der Löschfrist auf **vier Jahre**.
- In Anlehnung an die haushaltsrechtlichen Vorgaben der Sozialversicherung (SRVwV) beträgt die Aufbewahrung von Buchhaltungsdaten und Buchungsbelegen bis zu zehn Jahre, somit wird die Frist auf **zwölf Jahre** gesetzt.
- Die QSKH-RL enthält Verfahren mit Langzeitbetrachtungen, sogenannte Follow-Up Verfahren. Für diese ist es notwendig, die Leistungsempfänger über einen definierten Zeitraum von bis

zu acht Jahren zu verfolgen. Da die QS-Daten jedoch für die sekundäre Datennutzung zur Verfügung stehen sollen, werden diese Daten nach Abschluss des Follow-up Zeitraum nicht gelöscht, sondern gesperrt.

Mit dem Erreichen der Löschfrist muss die Löschung der Daten erfolgt sein.

2.4 Definition der Startzeitpunkte des Löschens

Ein genauer Zeitpunkt der Löschung ergibt sich erst aus der Frist und einem Startzeitpunkt. Hier werden folgende drei Startzeitpunkte definiert:

- Ab Erhebung
- Ab Ende des Vorgangs: ist ein Vorgang noch nicht abgeschlossen, können Daten ggf. noch gar nicht richtig beurteilt werden. In dem Fall soll die Löschfrist erst nach dem Ende des Vorgangs beginnen.
- Ab Ende der Beziehung: die ist der Startzeitpunkt z. B. für das Ausscheiden einer Person aus Rollen, die eine Teilnahme am System erlaubt haben.

Bei QS-Verfahren gilt die Betrachtung als „Vorgang“. Die Löschfrist beginnt mit Abschluss des QS-Verfahren bzw. des Follow-up Zeitraums.

2.5 Definition der Löschklassen

Aus den Standardlöschfristen und einem Startzeitpunkt wird entsprechend der DIN-Norm die Bildung einer Matrix, in die alle Datenkategorien einsortiert werden können. Jede Kombination bildet eine Löschkategorie.

Tabelle 15: Matrix der Löschklassen

	Sofort	2 Monate	6 Monate	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Ab Erhebung			QS-Daten Bewerberdaten	Eingangsdatensätze mit besonderem Analysebedarf			
Ab Ende des Vorgangs	Fehlerhafte Eingangsdatensätze	Websitelogs, Betriebslogs				Handelsbriefe	Buchhaltungsdaten
Ab Ende der Beziehung	Kontaktdaten der Gremienmitglieder Stammdaten der Verfahrensteilnehmer bei Löschung auf Verlangen			Stammdaten der Verfahrensteilnehmer		Verträge	Kernstammdaten Personaldaten

2.6 Archivierung

Daten die nicht mehr benötigt werden, aber für einen bestimmten Zweck aufbewahrt werden müssen, werden archiviert/gesperrt (z. B. eine Rechnung über eine Lizenz). Nach dem Ablauf der Frist ist auch hier sicherzustellen, dass die Daten gelöscht werden.

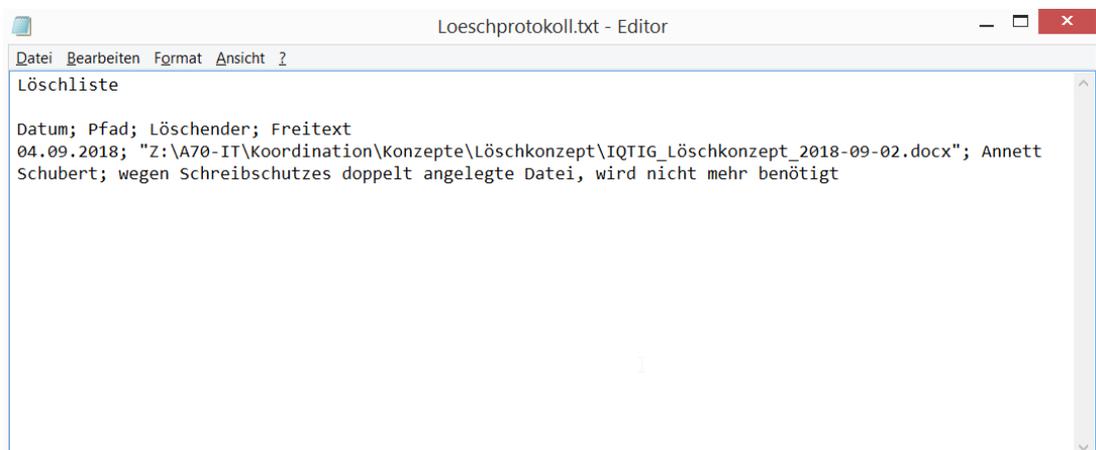
2.7 Durchführung der Löschung

Daten, für welche die Aufbewahrungsfrist abgelaufen ist, müssen gelöscht werden und mit dem Erreichen der Löschfrist gelöscht sein. Hierfür wird ein Verfahren entwickelt, das die Löschung nach manueller Bestätigung (4-Augen Prinzip) durchführt und ein Löschprotokoll erstellt. Das Löschverfahren sollte im Fehlerfall eine Meldung erzeugen, die dann manuell überprüft wird. Der Datenschutzbeauftragte prüft die Protokolle regelmäßig.

Folgende Löschmechanismen werden eingeführt:

- Beim Datenschutzbeauftragten wird eine Seite angelegt, auf der die Löschungen dokumentiert werden.
- Auf Systemen, in welchen oft Daten gelöscht werden wie z. B. Dateiablagen, kann die Löschung alternativ auch dadurch dokumentiert werden, dass im Wurzelverzeichnis der jeweiligen Ablage (Hier Z:\) eine Textdatei „Loeschprotokoll.txt“ angelegt wird. Dieses Protokoll ist ebenfalls beim Datenschutzbeauftragten aufzubewahren. Zu dokumentieren sind das Datum der Löschung, der Dateiname mit Pfad und Dateieindung, der Ausführende der Löschung und ggf. eine Bemerkung, als Trennzeichen ist ein Semikolon zu verwenden.

Abbildung 2: Löschprotokoll



- Löschpflichtige Daten, die auf dem E-Mail Server gespeichert sind, werden im E-Mail Programm manuell gelöscht und die Löschung protokolliert.
- Löschpflichtige Daten, die auf dem SFTP-Server gespeichert sind, werden dort manuell gelöscht und die Löschung protokolliert.
- Löschpflichtige Daten, die in Datenbanken gespeichert sind, werden durch entsprechende Routinen gelöscht. Der Löschvorgang wird dokumentiert.
- Löschpflichtige Daten, die auf dem Dateisystem gespeichert sind, werden manuell gelöscht und die Löschung protokolliert.

- Vor einer Löschung werden Suchmechanismen genutzt, um möglicherweise manuell erstellte Dubletten von Daten in den verteilten Systemen zu identifizieren.
- Physische Abbilder von Daten auf unveränderbaren Datenträgern (z. B. DVD, CD-Rom) werden mechanisch vernichtet. Veränderbare Datenträger (z. B. DVD, Festplatten) werden um die zu löschenden Daten bereinigt.
- In Backups bzw. Archiven werden ältere Datenbestände gesichert. Diese können ggf. Daten beinhalten, die in neuen Systemständen bereits gelöscht worden sind. Daher besteht das Risiko, dass bereits gelöschte Dateien durch eine Wiederherstellung des Systems wieder auferstehen. Als organisatorische Maßnahme wird deshalb definiert, dass nach einem Restore die in der beim Datenschutzbeauftragten vorliegenden Löschliste verzeichneten Ordner und Dateien sofort wieder gelöscht werden müssen.
- Es wird ein Automatismus erstellt, der nach Dubletten von Dateien sucht und diese automatisiert auswertet. Danach kann durch den Datenschutzbeauftragten und die betroffenen Abteilungen entschieden werden, an welcher Stelle eine Datei verbleibt und welche Kopien ggf. zu löschen sind.
- Es wird ein Automatismus erstellt, der nach Dateien mit typischen Bezeichnungen sucht. Danach kann der Datenschutzbeauftragte mit der betroffenen Abteilungen in Kontakt treten und ggf. Schulungsmaßnahmen durchführen sowie entscheiden, welche Dateien ggf. zu löschen sind. Diese Suchbegriffe sind insbesondere:
 - Dateien mit der Endung .xls und dem Namen „Kontakte“; „Bewerber“; „Kontaktliste“, „Passwörter“, „Kennwörter“
- Der Datenschutzbeauftragte kann der IT-Abteilung den Auftrag geben, Suchoperationen nach Suchbegriffen durchzuführen und ihm das Ergebnis zu liefern. Hier werden automatisierte Skripte eingesetzt.
- Die Abteilungen können ebenfalls eigene Löschlisten an geeigneter Stelle anlegen, in der sie die Aktivitäten gegenüber dem Datenschutzbeauftragten des IQTIG dokumentieren.

2.8 Dokumentation

Zum Nachweis sowohl der Integrität der Daten als auch der Integrität gemäß des Löschkonzepts wird ein jeder Löschvorgang dokumentiert.

Bei automatischen Löschvorgängen in Datenbanken wird automatisiert ein Protokoll erstellt. Bei manuellen Löschvorgängen wird ein Löschprotokoll manuell angelegt.

Dieses wird in Dateisystemen an einen festen Ort (Datenschutzbeauftragter) abgelegt, so dass im Backup- und Restore Fall geprüft werden kann, welche Daten auch nach der Wiederherstellung zwingend gelöscht worden sein müssen.

3 Sonderfälle

3.1 Löschung auf Verlangen

Nach Art. 17 DSGVO hat jede Person ein Recht auf „Vergessenwerden“. Macht er hiervon Gebrauch, so müssen Datensätze mit entsprechendem Bezug gelöscht werden. Gleiches gilt, wenn sich herausstellt, dass Daten rechtswidrig erhoben werden.

In diesem Fall dokumentiert das IQTIG den Auslöser indem es die Meldung an den Datenschutzbeauftragten weiter gibt, der die Löschung veranlasst. Solange bezüglich des Falls noch Klärungen notwendig sind, werden die Daten gesperrt und vor Veränderungen und Zugriff geschützt. Sollten die Datensätze an verschiedenen Stellen im IQTIG vorliegen, so fordert der Datenschutzbeauftragte auch diese Stellen zur Löschung auf und dokumentiert dies.

3.2 Vorgaben des IQTIG an Unternehmen, die im Auftrag Daten verarbeiten

Beauftragt das IQTIG Dritte mit der Verarbeitung von Daten werden im Rahmen der Beauftragung die Konzepte des IQTIG - konkret das Datenschutzkonzept und das Löschkonzept - dem Auftrag bzw. den Ausschreibungsunterlagen beigelegt, so dass deren Beachtung Teil des Auftrags wird. Bei besonderer Relevanz für das IQTIG soll ein potentieller Auftragnehmer im Angebot Stellung zum Löschverfahren nehmen und dies ist bei der Leistungsbewertung mit zu berücksichtigen.

Der Auftragsdatenverarbeiter wird zudem dahingehend vertraglich gebunden, dass er die Löschung dokumentiert und die Löschprotokolle an das IQTIG übergibt.

3.3 Umgang mit fehlerhaften Datenlieferungen

3.3.1 Im Rahmen des Aufbaus und der Erprobung von QS-Verfahren

Es kann im Rahmen des Aufbaus und der Erprobung der QS-Verfahren aus verschiedenen Gründen zu versehentlicher Übermittlung von personenbezogenen Daten kommen, obwohl keine Ermächtigungsgrundlage zur Verarbeitung dieser Daten existiert.

Würde man nun die Datensätze löschen und den Fehler zurückmelden, könnten ggf. Fristen zur Lieferung von Daten an das IQTIG verletzt werden. Daher wird das IQTIG bei Aufbau und Erprobung eines neuen QS-Verfahrens wie folgt vorgehen:

- Wird ein Fall bei der Prüfung entdeckt, stellt der Prüfer eine Hypothese und einen Vorgehensvorschlag auf.
- Diesen prüft er mit einem zweiten Bearbeiter (4-Augen Prinzip)
- Und nimmt dann eine Maßnahme der Datenbereinigung vor.

- Diese kann sein:
 - Schwärzen einer Textstelle in einem Binärdatendokument (z. B. gescannter QS-Bogen)
 - Löschen oder Ersetzen eines Texteintrags
- Information an die sendende Stelle über den Verstoß und Aufforderung zur Behebung des Fehlers.

Dadurch dass die sendende Stelle über den Verstoß informiert wird, wird eine Wiederholung der fehlerhaften Übermittlung unterbunden.

3.3.2 Im Regelbetrieb

Im Regelbetrieb werden die ohne Rechtsgrundlage übermittelten Daten zeitnah gelöscht, der Sender über die fehlerhafte Lieferung informiert und ggf. zur erneuten richtigen Lieferung aufgefordert.

4 Einführungsvorgehen

Das Löschkonzept findet in weiten Teilen bereits Anwendung. Richtlinien zur Verwendung von Daten in den einzelnen Fachabteilungen werden erarbeitet. Auf Basis dieser Richtlinien können Prozesse zur manuellen Löschung erstellt werden. Nachfolgend werden automatisierte Löschvorgänge geplant und getestet. Die Etablierung der automatischen Löschprozesse soll vor Ablauf der Zweckbindung der Daten der QS-Verfahren abgeschlossen sein.

Mit dem G-BA muss geklärt werden, wie die Löschvorgaben in den QS-Richtlinien und die Verpflichtung zur Vorhaltung der Daten für die sekundäre Datennutzung miteinander im Verhältnis stehen.

4.1 Planung

In einer Prozessbeschreibung wird definiert, welche Daten wann durch wen zu löschen sind.

4.2 Implementierung

Mit der Fertigstellung des Löschkonzeptes werden die Mechanismen zur Ermittlung zu löschender Daten umgesetzt. Die Löschlisten und Ablageorte für Löschprotokolle werden erstellt und eine Vorgabe zur Löschung für die Mitarbeiter des IQTIG erarbeitet.

Anschließend wird das Löschprozedere für die Mitarbeiter eingeführt, indem eine Arbeitsanweisung formuliert wird, die durch die Institutsleitung an alle Mitarbeiter per E-Mail gesendet wird und den Unterlagen für neue Mitarbeiter beigelegt wird. Durch Schulungsveranstaltungen werden die Mitarbeiter genauer informiert. Hier wird den Mitarbeitern u. a. erläutert, wie fragliche Fälle an den Datenschutzbeauftragten zu melden sind, der mit Ihnen zusammen entscheidet, wie im konkreten Fall zu verfahren ist. Diese Fälle werden als Liste im Intranet dokumentiert.

Als organisatorische Maßnahme wird ferner definiert, dass die Abteilungen einmal jährlich per E-Mail dazu aufgefordert werden, ihre Ablagen nach Daten zu durchsuchen, die nicht mehr aufbewahrt werden dürfen.

4.3 Test

Die Prozesse und Automatismen zur Löschung von Datensätzen werden einem ausführlichen Test unterzogen. Folgende Abläufe sind dabei mindestens Gegenstand des Tests:

- Erstellung eines Backups der Daten
- Vermerk eines Datensatzes für die Löschung
- 4-Augen Prüfung für die Veranlassung der Löschung
- Identifikation von Dubletten des Datensatzes
- Faktische Löschung
- Schreiben des Löschprotokolls (inkl. einer Liste der Daten, die nach dem Restore gelöscht werden müssen)
- Wiederherstellung des Backups

- Prüfung, dass die Daten nach der Wiederherstellung erneut gelöscht werden und die Löschprotokolle vorhanden sind
- Suche nach dem Datensatz schlägt fehl

Bei der Löschung eines Satzes aus der Teilnehmerdatenbank muss geprüft werden, dass eine Anmeldung mit dem Benutzer in den verschiedenen angeschlossenen Systemen sofort nicht mehr möglich ist.

4.4 Fortschreibung

Im Laufe der Datenverarbeitung kann es zu einer **Änderung des Zweckes** kommen. Hat das IQTIG z. B. Daten intern weiter gegeben und der Zweck für die Weitergabe entfällt, muss der Empfänger informiert und die Löschung veranlasst werden. Daher soll eine regelmäßige Revision des Konzepts und der Rechtsgrundlagen erfolgen.

Der Zeitraum hierfür wird auf zwölf Monate festgelegt.

Die neue DeQS-Richtlinie soll sukzessive die etablierten sektorenspezifischen QS-Verfahren weiterführen. Hier sollte regelmäßig und genau geprüft werden, ob durch den Übergang von Verfahren in die DeQS-RL sich Zwecke ändern und Daten ggf. anders behandelt werden müssen. Auch hier ist die abgeleitete Maßnahme eine regelmäßige Revision der Rechtsgrundlagen und des Konzepts.



ABNAHMEEMPFEHLUNG DATENSCHUTZKONZEPT IOTIG

Ergebnis der Begutachtung im Auftrag des Gemeinsamen Bundesausschusses

Stand 27. Februar 2019

Version 2.4

ZTG Zentrum für Telematik und Telemedizin GmbH

Universitätsstraße 142
44799 Bochum

T +49 (0) 234 . 97 35 17 – 0

F +49 (0) 234 . 97 35 17 – 30

E-Mail info@ztg-nrw.de

Internet www.ztg-nrw.de

ZTG Zentrum für Telematik und Telemedizin GmbH
Universitätsstraße 142 · 44799 Bochum
Telefon 0 234 . 97 35 17 - 0 · Fax 0 234 . 97 35 17 - 30
info@ztg-nrw.de URL: <http://www.ztg-nrw.de>
Geschäftsführer: Rainer Beckers M.P.H., M.A.
Dipl.-Soz.Wiss. Lars Treinat

Amtsgericht Bochum
HRB 13476
Bankverbindung:
Volksbank Bochum Witten
Kto.-Nr. 128 631 100
BLZ 430 601 29

ZTG ist Partner des



Hinweise zum Dokument

Die Verwendung und die Weitergabe des Dokumentes sind ausdrücklich auf die Nutzung im Zusammenhang der Beauftragung beschränkt. Es darf ohne Genehmigung der Autoren - auch auszugsweise - nicht reproduziert, übertragen, umgeschrieben oder weiterverbreitet werden.

Die ZTG GmbH sichert eine fundierte und gewissenhafte Ausführung der Begutachtung und Beratung zu. Die Einschätzung der jeweils zuständigen Aufsichtsbehörden kann sie jedoch nicht vorwegnehmen. Eine etwaige Haftung für Differenzen in der Bewertung kann der Auftragnehmer daher nicht übernehmen und wird generell ausgeschlossen. Die Verantwortung für die rechtskonforme Durchführung der Datenverarbeitung obliegt stets dem Verantwortlichen (vgl. Art. 4 Abs. 1 Nr. 7 EU-DSGVO).

Eine Rechtsberatung findet durch die ZTG GmbH nicht statt. Für eventuell im Dokument enthaltene rechtliche Interpretationen kann daher keine Gewähr übernommen werden.

1 Begutachtungsgegenstand

Begutachtet wurde das 26-seitige Dokument

„IQTIG Datenschutzkonzept v2.4“

mit angegebenem Stand vom 26. Februar 2019.

Zusätzlich wurden die in Kapitel 12 des Datenschutzkonzepts gelisteten 7 Anlagen beigefügt, die punktuell mitbetrachtet wurden.

2 Ergebnis der Begutachtung

In Anbetracht dessen, dass beim vorliegenden Datenschutzkonzept sowohl die wesentlichen Datenschutzaspekte adressiert sind als auch dass ein Datenschutzkonzept naturgemäß ein gelebtes Dokument ist, welches beim IQTIG gemeinsam mit der praktizierten Datenverarbeitung regelmäßig im Rahmen des integrierten Datenschutzmanagementsystems des IQTIG auf die aktuelle Berücksichtigung der Datenschutzerfordernungen überprüft und in den Details weiterentwickelt wird, sprechen wir in der Summe zum gegenwärtigen Zeitpunkt keine durchgreifenden Bedenken gegen eine Abnahme durch den Gemeinsamen Bundesausschuss aus.