Inhaltsverzeichnis

1 Definitionen

In diesen verbindlichen internen Datenschutzvorschriften haben die unten aufgeführten Begriffe jeweils die folgende Bedeutung:

i. „**Geltende Datenschutzgesetze**" bezeichnet die in einer Gerichtsbarkeit geltenden und auf eine Partei anwendbaren Datenschutzgesetze.

ii. „**Geltende Gesetze**" bezeichnet die in einer Gerichtsbarkeit geltenden und auf eine Partei anwendbaren Gesetze mit Ausnahme der geltenden Datenschutzgesetze.

iii. **„Verbindliche interne Datenschutzvorschriften"** bezeichnet dieses Dokument und dessen Anhänge.

iv. **„Verantwortlicher"** bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder in Zusammenarbeit mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.

v. „**Datenschutzberater**" bezeichnet den innerhalb der Fresenius-Gruppe zentral benannten Datenschutzberater.

vi. „**Datenschutz-Folgenabschätzung**" bezeichnet eine gezielt durchgeführte Risikobewertung zur Identifizierung, Beurteilung und Eindämmung der Datenschutzrisiken von Verarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen bergen könnten.

vii. „**Datenschutzbeauftragter**" bezeichnet den innerhalb der Fresenius-Gruppe benannten Datenschutzbeauftragten gemäß Artikel 37 DSGVO. Er darf bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhalten.

viii. „**Datenschutzorganisation**" bezeichnet jeweils die Datenschutzorganisation der einzelnen Parteien, bestehend aus einem oder mehreren (lokalen) Datenschutzberatern und (sofern gesetzlich vorgeschrieben) dem zuständigen Datenschutzbeauftragten.

ix. „**EWR**" bezeichnet den Europäischen Wirtschaftsraum.

x. „**Mitarbeiter**" bezeichnet alle Mitglieder des Managements einer Partei, alle Personen, die in einem Beschäftigungsverhältnis oder Quasi-Beschäftigungsverhältnis zu einer Partei stehen (darunter Zeitarbeiter, Lehrlinge, Auszubildende und Praktikanten) sowie Berater und alle sonstigen Personen, die in die Betriebsabläufe einer Partei integriert sind.

xi. „**EU**" bezeichnet die Europäische Union.

xii. „**Rahmenvereinbarung**" bezeichnet den Vertrag zwischen den Parteien über den Beitritt zu den verbindlichen internen Datenschutzvorschriften.

xiii. „**Fresenius-Gruppe**" bezeichnet im Rahmen dieser verbindlichen internen Datenschutzvorschriften die Fresenius SE & Co. KGaA („**FSE**") und alle verbundenen Unternehmen im Sinne von § 15ff. des deutschen Aktiengesetzes („**Fresenius-Unternehmen**"), mit Ausnahme aller zu den Geschäftssegmenten Fresenius Kabi, Fresenius Medical Care, Fresenius Helios und Fresenius Vamed gehörenden verbundenen Unternehmen. Des Weiteren umfasst der Begriff die Fresenius Kabi Aktiengesellschaft („**FK AG**") und alle verbundenen Unternehmen im Sinne von § 15ff. des deutschen Aktiengesetzes, die zum Geschäftssegment Fresenius Kabi gehören.

xiv. „**Weiterverarbeitung**" bezeichnet die Verarbeitung personenbezogener Daten durch eine Partei außerhalb der EU bzw. des EWR, wenn die personenbezogenen Daten ursprünglich durch eine an die DSGVO gebundene Partei übermittelt wurden.

xv. „**DSGVO**" bezeichnet die EU-Verordnung 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.

xvi. „**Betroffene Person**" bezeichnet eine identifizierte oder identifizierbare natürliche Person. 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen,

wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

xvii. „**Lokaler Datenschutzberater**" bezeichnet den innerhalb der Fresenius-Gruppe auf lokaler Ebene benannten lokalen Datenschutzberater.

xviii. „**Weiterübermittlung**" bezeichnet die Übermittlung personenbezogener Daten durch eine Partei außerhalb der EU bzw. des EWR an einen anderen Empfänger außerhalb der EU bzw. des EWR, wenn die personenbezogenen Daten ursprünglich durch eine an die DSGVO gebundene Partei übermittelt wurden.

xix. „**Partei**" oder „**Parteien**" bezeichnet die Unternehmen innerhalb der Fresenius-Gruppe, die an die verbindlichen internen Datenschutzvorschriften gebunden sind und in Anhang 1 aufgeführt sind.

xx. **„Personenbezogene Daten"** bezeichnet jede Information, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") bezieht. 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

xxi. „**Verarbeitung**" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, das Strukturieren, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

xxii. „**Verarbeiter**" bezeichnet eine interne oder externe natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

xxiii. „**Besondere Kategorien personenbezogener Daten**" bezeichnet personenbezogene Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

xxiv. „**Aufsichtsbehörde**" bezeichnet eine unabhängige Behörde, die von einem Mitgliedstaat gemäß Artikel 51 DSGVO eingerichtet wurde.

xxv. „**Zuständige Aufsichtsbehörde**" bezeichnet eine Aufsichtsbehörde, die für die Verarbeitung personenbezogener Daten durch eine Partei aus einem der folgenden Gründe zuständig ist:

- Die jeweilige Partei wurde im Staatsgebiet des Mitgliedstaates dieser Aufsichtsbehörde gegründet.
- Die jeweilige Partei hat ihre Hauptniederlassung oder ihre einzige Niederlassung im Staatsgebiet des Mitgliedstaates dieser Aufsichtsbehörde, von wo aus die Daten übermittelt wurden.
- Betroffene Personen, die ihren Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde haben, sind durch die Verarbeitung wesentlich berührt oder werden davon wahrscheinlich wesentlich berührt.
- Bei dieser Aufsichtsbehörde wurde eine Beschwerde eingereicht.

xxvi. „**Drittempfänger**" bezeichnet einen Empfänger personenbezogener Daten, der nicht an die verbindlichen internen Datenschutzvorschriften gebunden ist.

xxvii. „**Übermittlung**" bezeichnet jedwede Weitergabe personenbezogener Daten von einem Verantwortlichen an einen anderen Verantwortlichen, an einen Auftragsverarbeiter oder an einen anderen Empfänger.

Für Begriffe, die in diesem Abschnitt nicht definiert werden, gelten das Dokument Definition verbindliche interne Datenschutzvorschriften #16 und die Definitionen gemäß der DSGVO.

2 Ziel

Die Fresenius-Gruppe ist weltweit tätig. Dies schließt sowohl Länder mit geltenden Datenschutzgesetzen als auch Länder ohne geltende Datenschutzgesetze ein. Zur Vereinheitlichung des Umgangs mit und der Verarbeitung von personenbezogenen Daten innerhalb der Fresenius-Gruppe sowie zur Einhaltung der geltenden Datenschutzgesetze halten sich die an die verbindlichen internen Datenschutzvorschriften gebundenen Parteien an einen internen Katalog von verbindlichen internen Datenschutzvorschriften für die Verarbeitung personenbezogener Daten. Dadurch soll sichergestellt werden, dass in allen Parteien weltweit ein einheitliches und angemessenes Datenschutzniveau etabliert wird. Vornehmlicher Zweck der verbindlichen internen Datenschutzvorschriften ist die Harmonisierung des Datenschutzstandards innerhalb der Fresenius-Gruppe auf ein Datenschutzniveau, welches EU-Standards genügt. Eine solche Harmonisierung erlaubt den weltweiten Austausch personenbezogener Daten zwischen allen Parteien mit einem angemessenen Datenschutzniveau.

Entscheidende Akteure bei der Gewährleistung eines angemessenen Datenschutzniveaus sind in den einzelnen Fresenius-Unternehmen jeweils die Mitarbeitergruppen, die personenbezogene Daten verarbeiten. Ein angemessener Datenschutzstandard kann nur erreicht werden, wenn die betreffenden Mitarbeiter sich bewusst sind, wie personenbezogene Daten zu verarbeiten sind und welche Einschränkungen gelten.

In diesen verbindlichen internen Datenschutzvorschriften werden die grundlegenden Garantien der verbindlichen internen Datenschutzvorschriften formuliert. Ferner werden deren Anwendungsbereich, Ziele, Grundsätze und Struktur dargelegt.

3 Anwendungsbereich

3.1 Räumlicher Anwendungsbereich

i. Die verbindlichen internen Datenschutzvorschriften **finden Anwendung** in folgenden Szenarien:

- Verarbeitung personenbezogener Daten durch Parteien in der EU bzw. im EWR (einschließlich Übermittlungen an andere Parteien, unabhängig davon, ob sich die betreffenden Empfänger in der EU bzw. im EWR oder außerhalb befinden)
- Verarbeitung personenbezogener Daten durch Parteien außerhalb der EU bzw. des EWR, soweit eine solche Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung" der Fresenius-Gruppe in der EU bzw. im EWR erfolgt (einschließlich Übermittlungen an andere Parteien, unabhängig davon, ob sich die betreffenden Empfänger in der EU bzw. im EWR oder außerhalb befinden)[1]
- Verarbeitung personenbezogener Daten von betroffenen Personen in der EU bzw. im EWR durch Parteien außerhalb der EU bzw. des EWR, wenn die Verarbeitung in Zusammenhang damit steht, (i) Personen in der EU bzw. im EWR Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen Personen eine Zahlung zu leisten ist, oder (ii) das Verhalten von Personen zu beobachten, soweit das Verhalten in der EU bzw. im EWR erfolgt (einschließlich Übermittlungen an andere Parteien, unabhängig davon, ob sich die betreffenden Empfänger in der EU bzw. im EWR oder außerhalb befinden)
- Weiterverarbeitung personenbezogener Daten durch Parteien außerhalb der EU bzw. des EWR, soweit die betroffenen personenbezogenen Daten ursprünglich von einer an die DSGVO gebundenen Partei übermittelt wurden
- Weiterübermittlung personenbezogener Daten durch Parteien außerhalb der EU bzw. des EWR an einen anderen Empfänger außerhalb der EU bzw. des EWR, soweit die betroffenen personenbezogenen Daten ursprünglich von einer an die DSGVO gebundenen Partei übermittelt wurden

ii. Die verbindlichen internen Datenschutzvorschriften **finden keine Anwendung** auf die Verarbeitung personenbezogener Daten durch Parteien außerhalb der EU bzw. des EWR, wenn die Verarbeitung

- nicht „im Rahmen der Tätigkeiten einer Niederlassung" von Fresenius in der EU bzw. im EWR erfolgt.
- nicht im Zusammenhang damit steht, (i) Personen in der EU bzw. im EWR Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen Personen eine Zahlung zu leisten ist, oder (ii) das Verhalten von Personen zu beobachten, soweit das Verhalten in der EU bzw. im EWR erfolgt.
- keine personenbezogenen Daten betrifft, die ursprünglich von einer an die DSGVO gebundenen Partei übermittelt wurden.

3.2 Sachlicher und persönlicher Anwendungsbereich

i. Die verbindlichen internen Datenschutzvorschriften gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

ii. Die verbindlichen internen Datenschutzvorschriften gelten auch für Parteien, die personenbezogene Daten als (interner) Auftragsverarbeiter für ein anderes Fresenius-Unternehmen verarbeiten, jedoch nur in dem Maße, wie sie keiner gegenseitig getroffenen Vereinbarung widersprechen.

iii. Um Zweifel auszuschließen: Personenbezogene Daten dürfen gemäß den verbindlichen internen Datenschutzvorschriften nur zwischen Parteien übermittelt werden, welche die verbindlichen internen Datenschutzvorschriften ordnungsgemäß umgesetzt und bestätigt haben, dass sie erfolgreich Maßnahmen ergriffen haben, um die Einhaltung der verbindlichen internen Datenschutzvorschriften durchzusetzen.

iv. Die verbindlichen internen Datenschutzvorschriften gelten für die Verarbeitung personenbezogener Daten durch alle der unter „Anhang 1: Liste der an die verbindlichen internen Datenschutzvorschriften gebundenen Parteien" aufgeführten Parteien.

v. Die verbindlichen internen Datenschutzvorschriften umfassen im Grundsätzlichen die unter „Anhang 2: Arten von übermittelten personenbezogenen Daten" definierten Verarbeitungsvorgänge.

3.3 Beziehung zwischen den verbindlichen internen Datenschutzvorschriften und geltenden Datenschutzgesetzen

Alle Parteien haben diese verbindlichen internen Datenschutzvorschriften zu beachten und einzuhalten, ungeachtet der Tatsache, dass geltende Datenschutzgesetze eventuell ein anderes oder niedrigeres Schutzniveau vorsehen. Nichtsdestotrotz haben die Parteien in dem Fall, dass die geltenden Datenschutzgesetze strengere Regeln für die Verarbeitung vorsehen, zusätzlich zu den verbindlichen internen Datenschutzvorschriften auch diese strengeren Regeln der geltenden Datenschutzvorschriften zu beachten.

3.4 Kollisionen zwischen geltendem Recht und den verbindlichen internen Datenschutzvorschriften

Alle Parteien, die an die DSGVO gebunden sind, müssen im Zuge ihrer Risikobewertung gemäß Abschnitt 7 vor der erstmaligen Übermittlung personenbezogener Daten an eine andere Partei außerhalb der EU bzw. des EWR prüfen, ob letztere in der Lage ist, die in den verbindlichen internen Datenschutzvorschriften vorgesehenen Garantien in der Praxis zu gewährleisten.

Falls eine Partei Grund hat zu glauben, dass die geltenden Gesetze oder die geltenden Datenschutzgesetze sie selbst oder eine andere Partei an der Einhaltung der verbindlichen internen Datenschutzvorschriften hindern oder dies die in den verbindlichen internen Datenschutzvorschriften vorgesehenen Standards wesentlich beeinträchtigen könnte, muss die betreffende Partei unverzüglich den zuständigen Datenschutzbeauftragten informieren, um die Auswirkungen zu bewerten und den Konflikt zu lösen. Der Datenschutzbeauftragte wiederum informiert als Beauftragter die EWR-Zentrale oder das EWR-Unternehmen.

Wenn eine rechtliche Vorgabe wie beispielsweise eine einer Partei erteilte verbindliche Anordnung zur Offenlegung personenbezogener Daten wesentliche negative Auswirkungen für die Garantien hat, welche die Fresenius-Gruppe durch die verbindlichen internen Datenschutzvorschriften eingerichtet hat, muss die betreffende Partei dieses Problem dem lokalen Datenschutzberater

melden und dabei die angeforderten Daten, die Identität der anfordernden Stelle sowie die Rechtsgrundlage angeben. Der lokale Datenschutzberater wird den zuständigen Datenschutzbeauftragten informieren, der wiederum als Beauftragter die EWR-Zentrale oder das EWR-Unternehmen informiert. Die Aufsichtsbehörde in Hessen, Deutschland, wird vom zuständigen Datenschutzbeauftragten informiert. Alle Informationen sind ohne schuldhaftes Zögern zur Verfügung zu stellen.

Falls eine solche Mitteilung durch geltende Gesetze verboten ist, bemüht sich die Partei nach besten Kräften, die erforderliche Genehmigung einzuholen, um den zuständigen Datenschutzbeauftragten und anschließend die Aufsichtsbehörde in Hessen, Deutschland, so schnell und umfangreich wie möglich zu informieren.

Wenn es einer Partei nicht erlaubt ist, spezifische Informationen zu einer Anfrage zu liefern, legt diese Partei dem zuständigen Datenschutzbeauftragten jährlich allgemeine Informationen mit dem größtmöglichen Umfang an relevanten Angaben über eingegangene Anfragen vor (wobei insbesondere die Anzahl der eingegangenen und befolgten Offenlegungsanordnungen, die anfordernden Stellen, die betroffenen Kategorien betroffener Personen und die Arten personenbezogener Daten anzugeben sind), um die Information der Aufsichtsbehörde in Hessen, Deutschland, zu ermöglichen.

In jedem Fall dürfen Übermittlungen personenbezogener Daten durch eine Partei an öffentliche Behörden nicht in einer Weise umfangreich, unverhältnismäßig und willkürlich sein, die über die Erfordernisse in einer demokratischen Gesellschaft hinausgeht.

4 Verbindlichkeit der verbindlichen internen Datenschutzvorschriften/Drittbegünstigtenrechte

Die verbindlichen internen Datenschutzvorschriften sind bindend für alle Parteien und deren Mitarbeiter. Betroffene Personen sind Drittbegünstigte und können Rechte aus den verbindlichen internen Datenschutzvorschriften ableiten. Alle Parteien sowie alle ihre Mitarbeiter sind zur Einhaltung der in den verbindlichen internen Datenschutzvorschriften formulierten Grundsätze und Pflichten verpflichtet.

Die Verbindlichkeit der verbindlichen internen Datenschutzvorschriften umfasst Folgendes:

i. *Verbindlichkeit für die Parteien*: Die Fresenius-Gruppe hat die verbindlichen internen Datenschutzvorschriften innerhalb der Parteien eingeführt und einen Mechanismus implementiert, der die verbindlichen internen Datenschutzvorschriften bindend macht für alle unter „Anhang 1: Liste der an die verbindlichen internen Datenschutzvorschriften gebundenen Parteien" aufgeführten Parteien. Jedes Fresenius-Unternehmen hat sich durch die Unterzeichnung der gemeinsamen Rahmenvereinbarung mit allen gebundenen Parteien vertraglich zur Einhaltung der in den verbindlichen internen Datenschutzvorschriften formulierten Grundsätze verpflichtet. Sofern für das Inkrafttreten der verbindlichen internen Datenschutzvorschriften notwendig, muss jede Partei sämtliche zusätzlich erforderlichen Voraussetzungen erfüllen, um die verbindlichen internen Datenschutzvorschriften gemäß Vertrag verbindlich zu machen.

ii. *Verbindlichkeit für Mitarbeiter*: Mitarbeiter sind zur Einhaltung der in den verbindlichen internen Datenschutzvorschriften formulierten Grundsätze verpflichtet. Diese Verpflichtung ergibt sich aus den allgemeinen Verpflichtungen zur Einhaltung von Unternehmensrichtlinien, die in ihrem Arbeitsvertrag festgeschrieben sind. Die Durchsetzung der verbindlichen internen Datenschutzvorschriften sowie möglicher Mitarbeitersanktionen aufgrund von Verstößen gegen die verbindlichen internen Datenschutzvorschriften wird durch die interne Compliancestruktur gewährleistet. Sofern für die Verbindlichkeit der verbindlichen internen Datenschutzvorschriften für die Mitarbeiter notwendig, muss jede Partei sämtliche zusätzlich erforderlichen Voraussetzungen erfüllen, um die verbindlichen internen Datenschutzvorschriften gemäß Vertrag verbindlich zu machen.

iii. *Verbindlichkeit für betroffene Personen (Drittbegünstigtenrechte)*: Alle Parteien verpflichten sich dazu, betroffenen Personen im Rahmen der verbindlichen internen Datenschutzvorschriften Drittbegünstigtenrechte hinsichtlich der Verarbeitung personenbezogener Daten zu gewähren. Demgemäß erkennt jede Partei ausdrücklich an und stimmt ausdrücklich zu, dass betroffene Personen berechtigt sind, die Bestimmungen der

Abschnitte 3.3, 3.4,4, 6.1-6.8, 9.1-9.7 und 10.1-10.4 dieser verbindlichen internen Datenschutzvorschriften hinsichtlich der Verarbeitung sie betreffender personenbezogener Daten sowie die weiteren Bestimmungen in Abschnitt 10 durchzusetzen.

5 Datenschutzorganisation

Die Fresenius-Gruppe hat eine interne Datenschutzorganisation eingerichtet und innerhalb der Parteien Rollen und Verantwortlichkeiten zugewiesen, um ein angemessenes Governance- und Supportframework zu etablieren und die rechtmäßige Verarbeitung personenbezogener Daten zu gewährleisten. Der Fresenius-Konzern wird bei Bedarf einen Datenschutzbeauftragten benennen und die Datenschutzorganisation aufrechterhalten, um eine angemessene Steuerung und Unterstützung für jede Partei wie folgt fortzusetzen:

- Der Datenschutzbeauftragte überwacht, beurteilt und prüft die Einhaltung der verbindlichen internen Datenschutzvorschriften und der geltenden Datenschutzgesetze, Datenschutzrichtlinien und Datenschutzverfahren. Der Datenschutzbeauftragte informiert und berät die Parteien und ihre Mitarbeiter hinsichtlich ihrer Pflichten unter den verbindlichen internen Datenschutzvorschriften und den geltenden Datenschutzgesetzen und spricht auf Aufforderung Empfehlungen aus. Im Rahmen von Datenschutz-Folgenabschätzungen untersucht er Verstöße und überwacht deren Behebung, macht Vorschläge zur Verbesserung des Datenschutzmanagementsystems, kooperiert mit Aufsichtsbehörden und fungiert als deren primärer Ansprechpartner. Der Datenschutzbeauftragte hat den bei seiner Ernennung definierten Zuständigkeitsbereich und berichtet direkt an das oberste Management. In dieser Rolle agiert der Datenschutzbeauftragte unabhängig.
- Der Datenschutzberater ist innerhalb der Datenschutzorganisation unterstützend und beratend tätig und zuständig für die Erstellung, Bereitstellung und Pflege des Datenschutzmanagementsystems, um die rechtmäßigen Verarbeitung personenbezogener Daten und die Einhaltung der verbindlichen internen Datenschutzvorschriften und der geltenden Datenschutzgesetze zu ermöglichen. Ferner prüft der Datenschutzberater die innerhalb der Fresenius-Gruppe zum Einsatz kommenden Konzepte für die Verarbeitung personenbezogener Daten, führt Datenschutzrisikobewertungen durch, berät hinsichtlich Datenverarbeitungsvereinbarungen, unterstützt Geschäftsprozesseigner bei der Aufzeichnung aller Datenverarbeitungsaktivitäten, berät bei Datenschutz-Folgenabschätzungen, beantwortet Anfragen betroffener Personen und trägt dafür Sorge, dass die lokalen Datenschutzberater fachkundige Beratung leisten können.

  Sofern erforderlich unterstützt der Datenschutzberater den Datenschutzbeauftragten auf Aufforderung bei dessen Überwachungsaufgaben und fungiert als Ansprechpartner für die Aufsichtsbehörden (beispielsweise zur Überwindung von Sprachbarrieren).
- Der lokale Datenschutzberater berät und unterstützt Geschäftsprozesseigner hinsichtlich aller Aktivitäten des jeweiligen lokalen Fresenius-Unternehmens oder hinsichtlich eines bestimmten Themenbereichs, hilft bei Sprachproblemen, führt für das lokale Unternehmen bzw. für den jeweiligen Themenbereich relevante Risikobewertungen durch und prüft alle zur Anwendung kommenden Datenverarbeitungskonzepte und Datenverarbeitungsvereinbarungen. Er unterstützt den Geschäftsprozesseigner bei der Pflege das Verzeichnisses der Datenverarbeitungsaktivitäten sowie der Dokumentation aller implementierten Datenschutzmaßnahmen.

  Sofern erforderlich unterstützt der lokale Datenschutzberater den Datenschutzberater und den Datenschutzbeauftragten.

  Lokale Datenschutzberater werden ausschließlich innerhalb der FK AG ernannt.

Der **Datenschutzbeauftragte der FSE** und der verbundenen Unternehmen im Sinne von § 15ff. des deutschen Aktiengesetzes, ausgenommen die zu den Unternehmenssegmenten Fresenius Kabi, Fresenius Medical Care, Fresenius Helios und Fresenius Vamed gehörenden verbundenen Unternehmen, ist wie folgt erreichbar:

Datenschutzbeauftragter Fresenius SE & KGaA

Fresenius SE & Co. KGaA
Else-Kröner-Str. 1
61352 Bad Homburg vor der Höhe
Deutschland
dataprotectionofficer@fresenius.com

Der **Datenschutzbeauftragte der FK AG** und der verbundenen Unternehmen im Sinne von § 15ff. des deutschen Aktiengesetzes, die zum Unternehmenssegment Fresenius Kabi gehören, ist wie folgt erreichbar:

Datenschutzbeauftragter Fresenius Kabi

Fresenius Kabi AG
Else-Kröner-Str. 1
61352 Bad Homburg vor der Höhe
Deutschland
dataprotectionofficer@fresenius-kabi.com

6 Datenschutzgrundsätze der verbindlichen internen Datenschutzvorschriften

Die Parteien erkennen die Bedeutung der Privatsphäre natürlicher Personen an. Bei der Verarbeitung personenbezogener Daten im Besitz der Parteien sind die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen, insbesondere das Recht auf den Schutz personenbezogener Daten.

Im Rahmen des Anwendungsbereichs dieser verbindlichen internen Datenschutzvorschriften verpflichtet sich jede Partei zur Einhaltung der folgenden Grundsätze für die Verarbeitung personenbezogener Daten:

6.1 Rechtmäßigkeit

Die Parteien verarbeiten personenbezogene Daten ausschließlich auf rechtmäßige Art und Weise. Die genaue rechtliche Grundlage jeder Datenverarbeitungsaktivität ist zu dokumentieren.

Die Parteien werden personenbezogene Daten nur verarbeiten, wenn einer der folgenden rechtlichen Gründe gegeben ist:

i. Es liegt eine Einwilligung der betroffenen Person vor, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere festgelegte Zwecke einverstanden ist.

ii. Die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen.

iii. Die Verarbeitung ist erforderlich zur Erfüllung der rechtlichen Verpflichtungen der Fresenius-Gruppe, beispielsweise steuerrechtlicher Verpflichtungen oder Verpflichtungen hinsichtlich der Arzneimittelüberwachung oder des Beobachtungs- und Meldesystems für Medizinprodukte.

iv. Die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der betreffenden Partei übertragen wurde.

v. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

vi. Die Verarbeitung ist erforderlich zur Wahrung eines berechtigten Interesses der betreffenden Partei oder eines Dritten, sofern nicht das Interesse der betroffenen Person überwiegt, die Verarbeitung sie betreffender personenbezogener Daten zu unterbinden (siehe 9.6).

Die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln im Rahmen der oben angeführten rechtlichen Gründe dürfen nur unter Aufsicht einer Aufsichtsbehörde vorgenommen werden oder wenn die Verarbeitung nach geltenden Datenschutzgesetzen, die geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorsehen, zulässig ist. Abschnitt 3.4 bleibt unberührt.

Die geltenden Datenschutzgesetze und die geltenden Gesetze formulieren möglicherweise zusätzliche oder abweichende Bestimmungen für die Verarbeitung personenbezogener Daten von Mitarbeitern. In diesem Fall werden die Parteien die betreffenden Bestimmungen bei der Verarbeitung personenbezogener Daten von Mitarbeitern einhalten. Abschnitt 3.3 und 3.4 bleiben unberührt.

Die Parteien werden besondere Kategorien personenbezogener Daten nur verarbeiten, wenn einer der folgenden rechtlichen Gründe gegeben ist:

i. Die betroffene Person hat in die Verarbeitung solcher personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt.

ii. Die Verarbeitung ist für Beschäftigungs- oder Sozialversicherungszwecke erforderlich.

iii. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben.

iv. Die betroffene Person hat die personenbezogenen Daten offensichtlich öffentlich gemacht.

v. Die Verarbeitung ist erforderlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

vi. Die Verarbeitung ist erforderlich aus Gründen eines erheblichen öffentlichen Interesses und steht in angemessenem Verhältnis zum verfolgten Ziel, wahrt den Wesensgehalt des Rechts auf Datenschutz und sieht angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vor.

vii. Die Datenverarbeitung ist erforderlich für präventivmedizinische oder arbeitsmedizinische Zwecke, für die Beurteilung der Arbeitsfähigkeit von Mitarbeitern, medizinische Diagnosen, die Bereitstellung von Gesundheitsversorgung und Sozialfürsorge oder Behandlung oder die Verwaltung von Gesundheits- und Sozialsystemen und -dienstleistungen.

viii. Die Verarbeitung ist erforderlich aus Gründen des öffentlichen Interesses im Bereich der öffentlichen (grenzüberschreitenden) Gesundheit wie der Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, und wahrt die Rechte der betroffenen Personen, insbesondere das Berufsgeheimnis.

ix. Die Verarbeitung ist erforderlich für im öffentlichen Interesse liegende Archivierungszwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, vorausgesetzt, dass die Verarbeitung den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person sowie der Grundsätze dieser verbindlichen internen Datenschutzvorschriften vorsieht.

6.2 Transparenz und Verarbeitung nach Treu und Glauben

Alle Parteien müssen personenbezogene Daten nach Treu und Glauben und in nachvollziehbarer Weise verarbeiten. Betroffene Personen sind grundsätzlich und in angemessener Weise vorab über die Verarbeitung sie betreffender personenbezogener Daten zu informieren. Ferner sind die betroffenen Personen über ihre Rechte als betroffene Personen gemäß Abschnitt 9 unten sowie alle sonstigen Rechte bezüglich sie betreffender personenbezogener Daten, die ihnen auf Grundlage des geltenden Rechts zustehen, zu informieren (siehe Abschnitt 9 unten).

Wenn die personenbezogenen Daten nicht von der betroffenen Person selbst bereitgestellt werden, erfolgt die Information:

i. innerhalb einer angemessenen Frist nach der Erhebung der personenbezogenen Daten, spätestens jedoch innerhalb eines Monats; unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten verarbeitet werden

ii. wenn die personenbezogenen Daten für die Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt des ersten Kontakts mit der betroffenen Person

iii. wenn die Offenlegung gegenüber einem anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung der personenbezogenen Daten

Alle Informationen oder Mitteilungen, die sich auf die Verarbeitung personenbezogener Daten betroffener Personen beziehen, sind den betroffenen Personen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

6.2.1 Verpflichtende Informationen

Die an betroffene Personen übermittelten transparenten Informationen müssen Folgendes enthalten:

i. den Namen und die Kontaktdaten der Partei sowie gegebenenfalls des Vertreters des Fresenius-Unternehmens

ii. die Kontaktdaten des Datenschutzbeauftragten (sofern benannt)

iii. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage der Verarbeitung

iv. wenn die Verarbeitung auf berechtigten Interessen beruht, die berechtigten Interessen, die von der Partei oder einem Drittempfänger verfolgt werden

v. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

vi. jede Übermittlung personenbezogener Daten in ein Land außerhalb der EU bzw. des EWR oder an eine internationale Organisation, die Rechtsgrundlage, auf der die Übertragung basiert, einschließlich der Angabe der angemessenen oder geeigneten Garantien und der Information, wie eine Kopie dieser Garantien angefordert werden kann oder wo sie verfügbar sind.

6.2.2 Zusätzliche Informationen, die bereitgestellt werden müssen

Im Sinne der Gewährleistung einer transparenten Verarbeitung nach Treu und Glauben sind zudem die folgenden zusätzlichen Informationen zur Verfügung zu stellen:

i. die Dauer, für die die personenbezogenen Daten gespeichert werden

ii. die Rechte betroffener Personen gemäß Abschnitt 9 dieser verbindlichen internen Datenschutzvorschriften

iii. wenn die Verarbeitung auf einer Einwilligung gründet, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, anwendbar ausschließlich auf die zukünftige Verarbeitung personenbezogener Daten

iv. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

v. den Einsatz automatisierter Entscheidungsfindung einschließlich Profiling sowie aussagekräftige Informationen über die zugrundeliegende Logik und die beabsichtigten Folgen der Verarbeitung.

vi. ob die Bereitstellung personenbezogener Daten eine gesetzliche oder vertragliche Anforderung oder eine für einen Vertragsabschluss notwendige Anforderung darstellt und ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, sowie die möglichen Konsequenzen, wenn die Bereitstellung der Daten verweigert wird

6.2.3 Zusätzliche Informationen, die bereitgestellt werden müssen, wenn Daten von einem Dritten erhoben werden

Wenn personenbezogene Daten von einem Dritten erhoben werden, der nicht die betroffene Person ist, stellt die Partei zusätzlich folgende Informationen bereit:

i. die Kategorien von verarbeiteten personenbezogenen Daten

ii. die Quelle der personenbezogenen Daten

6.3 Zweckbindung

Die Parteien dürfen personenbezogene Daten ausschließlich für die festgelegten Zwecke verarbeiten, für die die personenbezogenen Daten erhoben werden. Es ist den Parteien untersagt, personenbezogene Daten für Zwecke zu verarbeiten, die mit den ursprünglichen Zwecken nicht vereinbar sind. Eine Änderung des Zwecks ist nur zulässig, soweit sie von den EU-Datenschutzgesetzen abgedeckt ist. Zum Schutz der Rechte und Freiheiten betroffener Personen werden weitere Maßnahmen ergriffen, darunter die Einholung der Einwilligung der jeweils betroffenen Personen, die Einschränkung des Zugriffs auf die personenbezogenen Daten, zusätzliche Vertraulichkeits- und Sicherheitskontrollen sowie die Übermittlung von Informationen an die betroffenen Personen.

Grundsätzlich zulässige Zwecke für eine Weiterverarbeitung, die als mit dem ursprünglichen Zweck vereinbar angesehen werden, sind:

i. Archivierung

ii. interne Audits und Untersuchungen

Um festzustellen, ob die Verarbeitung zu einem anderen Zweck vereinbar ist mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, ist unter anderem Folgendes zu berücksichtigen:

i. jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung

ii. der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und der jeweiligen Partei

iii. die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO verarbeitet werden

iv. die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen

v. das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann

Der (lokale) Datenschutzberater kann hinsichtlich der Frage beraten, ob und wann eine solche Änderung zulässig ist.

Ist eine Änderung des Zwecks zulässig, müssen die betroffenen Personen gemäß Abschnitt 6.2 über die Änderung informiert werden, bevor die personenbezogenen Daten zu diesen anderen Zweck verarbeitet werden.

6.4 Datenminimierung

Jede Partei erhebt und verarbeitet personenbezogene Daten nur im erforderlichen Umfang für den Geschäftszweck, über den die betroffene Person informiert wurde (ursprünglicher Zweck), oder für Zwecke, die gemäß Abschnitt 6.3 mit diesen ursprünglichen Zwecken kompatibel sind. Es ist den Parteien untersagt, personenbezogene Daten zu erheben und zu verarbeiten, die über das notwendige Maß für den Zweck, für den sie benötigt werden, hinausgehen oder für diesen Zweck unerheblich sind.

6.5 Richtigkeit

Die Fresenius-Gruppe trägt Sorge dafür, dass personenbezogene Daten sachlich richtig und auf dem neuesten Stand sind. Alle Parteien treffen Maßnahmen, damit während des gesamten Datenlebenszyklus unrichtige Daten unverzüglich gelöscht, berichtigt oder aktualisiert werden.

6.6 Speicherbegrenzung

Die Parteien speichern personenbezogene Daten nur so lange, wie es für den Zweck, für den sie verarbeitet werden, erforderlich ist, es sei denn, die personenbezogenen Daten müssen aus gesetzlichen Gründen aufbewahrt werden. Ist die Aufbewahrung der personenbezogenen Daten aus anderen Gründen erforderlich als für den ursprünglichen Zweck (z. B. aufgrund gesetzlicher

Vorschriften über längere Aufbewahrungsfristen), wird der Zugriff auf die Daten eingeschränkt. Sobald aufseiten der Partei nicht länger ein rechtliches oder berechtigtes Interesse zur Speicherung der personenbezogenen Daten besteht, werden die personenbezogenen Daten anonymisiert oder sicher gelöscht.

6.7 Sicherheit, Integrität und Vertraulichkeit

6.7.1 Technische und organisatorische Sicherheitsmaßnahmen

Alle Parteien ergreifen angemessene technische und organisatorische Maßnahmen, um personenbezogene Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, vor unbeabsichtigter oder unrechtmäßiger Vernichtung, unbeabsichtigtem Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu schützen. Jede Partei hat bei der Umsetzung dieser technischen und organisatorischen Maßnahmen den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten betroffener Personen zu berücksichtigen. Zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit gespeicherter personenbezogener Daten werden Datenverarbeitungssysteme und Datenverarbeitungsdienste eingerichtet und gepflegt, die dauerhaft gegen Cybersicherheitsangriffe und IT-Sicherheitsbedrohungen abgesichert sind. Weitere Maßnahmen sind unter anderem die Folgenden:

i. die Pseudonymisierung und Verschlüsselung personenbezogener Daten

ii. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

iii. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

iv. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

6.7.2 Benachrichtigung über Datenschutzverletzungen

Alle Parteien sind verpflichtet, die Datenschutzorganisationen der FSE und der FK AG über jedwede Verletzung der Sicherheit zu informieren, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum unbeabsichtigten Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt. Die Datenschutzorganisationen haben sodann die EWR-Zentrale zu informieren. Zusätzlich bestehen im Falle einer Datenschutzverletzung die folgenden Benachrichtigungspflichten:

i. Jede Partei, die der DSGVO untersteht und als Verantwortlicher agiert, muss jede Datenschutzverletzung, die ein Risiko für die betroffenen Personen mit sich bringen könnte, unverzüglich und, sofern machbar, nicht später als zweiundsiebzig (72) Stunden nach Bekanntwerden der Datenschutzverletzung der Aufsichtsbehörde melden.

ii. Jede andere Partei, die als Verantwortlicher agiert, muss jede Datenschutzverletzung, die ein Risiko für die betroffenen Personen mit sich bringen könnte, unverzüglich und, sofern machbar, nicht später als zweiundsiebzig (72) Stunden nach Bekanntwerden der Datenschutzverletzung der zuständigen Aufsichtsbehörde melden.

iii. Jede Partei, die für eine andere Partei als Auftragsverarbeiter agiert, muss jede Datenschutzverletzung der als Verantwortlicher agierenden Partei und dem zuständigen lokalen Datenschutzberater melden.

iv. Wenn die Wahrscheinlichkeit besteht, dass eine Datenschutzverletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, muss die im jeweiligen Fall als Verantwortlicher agierende Partei die betroffenen Personen unverzüglich über die Datenschutzverletzung informieren.

Alle Parteien dokumentieren sämtliche festgestellten Verletzungen der Sicherheit (einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, der Auswirkungen der Verletzung und der ergriffenen Abhilfemaßnahmen). Die Dokumentation wird nach Rücksprache mit der Datenschutzorganisation der FSE und der FK AG an die Aufsichtsbehörden übermittelt.

6.8 Rechenschaftspflicht

Alle Parteien haben die vorstehend formulierten Grundsätze zu beachten und müssen die Einhaltung der verbindlichen internen Datenschutzvorschriften nachweisen können. Zu diesem Zweck ist eine angemessene Dokumentation zu erstellen und zu pflegen, einschließlich Folgendem:

i. Verzeichnis von Verarbeitungstätigkeiten, das folgende Angaben enthält:

- die Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie des Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten außerhalb der EU oder an eine internationale Organisation, einschließlich geeigneter Garantien gemäß Abschnitt 6.8.2
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Abschnitt 6.7

Das Verzeichnis ist schriftlich zu führen, was auch in elektronischem Format erfolgen kann, und ist Aufsichtsbehörden auf Anfrage zur Verfügung zu stellen.

ii. Implementierung angemessener technischer und organisatorischer Maßnahmen zur Umsetzung der Datenschutzgrundsätze und zur Gewährleistung der Einhaltung der Vorgaben in den geltenden verbindlichen internen Datenschutzvorschriften (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)

iii. Durchführung von Datenschutz-Folgenabschätzungen gemäß Abschnitt 8

6.8.1 Beauftragung von Auftragsverarbeitern

Die Parteien beauftragen ausschließlich Auftragsverarbeiter, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der verbindlichen internen Datenschutzvorschriften und der geltenden Datenschutzgesetze (insbesondere der DSGVO) erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.

Jede Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet. Ein solcher Vertrag bzw. ein solches anderes Instrument sieht unter anderem Folgendes vor:

i. Der Auftragsverarbeiter darf personenbezogene Daten ausschließlich im Rahmen der vom Datenverantwortlichen erhaltenen Weisungen verarbeiten.

ii. Der Auftragsverarbeiter muss angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten aufrechterhalten.

iii. Der Auftragsverarbeiter stellt sicher, dass Personen, die befugt sind, personenbezogene Daten zu verarbeiten, sich zur Vertraulichkeit verpflichtet haben oder einer geeigneten gesetzlichen Vertraulichkeitsverpflichtung unterstehen.

iv. Der Auftragsverarbeiter muss alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen entweder löschen oder zurückgeben und vorhandene Kopien löschen.

v. Der Auftragsverarbeiter darf ausschließlich solche Unterauftragsverarbeiter beauftragen, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der verbindlichen internen Datenschutzvorschriften und der geltenden

Datenschutzgesetze erfolgt. Es ist ein schriftlicher Vertrag abzuschließen, der dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt, die zwischen der Partei und dem Auftragsverarbeiter vereinbart sind.

vi. Der Auftragsverarbeiter unterstützt die jeweilige Partei bei der Erfüllung ihrer Verpflichtung, Anfragen betroffener Personen zu beantworten.

vii. Der Auftragsverarbeiter stellt alle Informationen zur Verfügung, die notwendig sind, um die Einhaltung dieses Abschnitts zu belegen, und gestattet Audits einschließlich Inspektionen der jeweiligen Partei oder eines anderen vereinbarten Prüfers.

viii. Der Auftragsverarbeiter unterstützt die jeweilige Partei bei der Sicherstellung der Pflichterfüllung, wie in Abschnitt 6.7 und 7 erwähnt.

6.8.2 Übermittlungen und Weiterübermittlungen personenbezogener Daten

Die Parteien treffen Maßnahmen zur angemessenen Absicherung von Übermittlungen personenbezogener Daten an Drittempfänger außerhalb des EWR in Übereinstimmung mit den vorliegenden verbindlichen internen Datenschutzvorschriften.

Personenbezogene Daten dürfen nur an einen Drittempfänger außerhalb des EWR übermittelt werden, wenn mindestens eine der folgenden Bedingungen zutrifft:

i. Der Drittempfänger befindet sich in einem Land, das laut Beschluss der Europäischen Kommission ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet (einem sogenannten Whitelist-Land), und erfüllt gegebenenfalls alle zusätzlichen Bestimmungen der jeweils geltenden Angemessenheit.

ii. Der Drittempfänger hat geeignete Garantien vorgesehen, und betroffenen Personen stehen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung, beispielsweise in Gestalt von Standardvertragsklauseln, die von der EU-Kommission verabschiedet wurden.

Als Ausnahme von den zuvor genannten Alternativen können personenbezogene Daten auch dann übermittelt werden, wenn einer der folgenden Fälle zutrifft:

i. Die betroffene Person hat der Übermittlung ihrer personenbezogenen Daten ausdrücklich zugestimmt, nachdem sie über die möglichen Risiken der Übermittlung informiert wurde.

ii. Die Übermittlung der personenbezogenen Daten ist erforderlich (i) für die Erfüllung eines Vertrags mit der betroffenen Person oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person oder (ii) zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags.

iii. Die Übermittlung der personenbezogenen Daten ist erforderlich (i) zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen (z. B. bei Entscheidungen über Leben und Tod), sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, oder (ii) zur Geltendmachung, Ausübung oder Verteidigung eines Rechtsanspruchs durch Fresenius oder (iii) aus wichtigen Gründen des öffentlichen Interesses.

iv. Die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der EU oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur, soweit die im Recht der EU oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Wenn keine der oben angeführten Bedingungen zutrifft und die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung zwingender berechtigter Interessen erforderlich ist und die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, beurteilt die übermittelnde Partei die Umstände der Datenübermittlung und gibt geeignete Garantien in Bezug auf den Schutz der personenbezogenen Daten. Anschließend setzt die übermittelnde Partei die Aufsichtsbehörde von der Übermittlung in Kenntnis.

Vorsorglich wird angemerkt, dass die vorgenannten Bedingungen auch für alle Weiterübermittlungen personenbezogener Daten durch Parteien außerhalb der EU bzw. des EWR an einen Drittempfänger außerhalb der EU bzw. des EWR gelten, soweit die betroffenen

personenbezogenen Daten ursprünglich von einer Partei in der EU bzw. im EWR übermittelt wurden.

7 Datenschutzrisikobewertung

Alle Parteien führen für jede mit personenbezogenen Daten in Zusammenhang stehende Datenverarbeitungsaktivität eine Datenschutzrisikobewertung durch. Eine Datenschutzrisikobewertung ist ein formaler Prozess zur Beurteilung der Folgen einer Datenverarbeitungsaktivität für die Rechte und Freiheiten der jeweiligen betroffenen Personen (Datenschutzrisiken). Die Risikobewertung besteht aus einer detaillierten Analyse der Datenverarbeitungsaktivität und dient der Identifizierung von Folgendem:

i. Datenschutzrisiken für betroffene Personen, welche die Datenverarbeitungsaktivität birgt

ii. geltende Anforderungen aufgrund der verbindlichen internen Datenschutzvorschriften und der geltenden Datenschutzgesetze

iii. angemessenen Maßnahmen zur Erfüllung dieser Anforderungen und zur Eindämmung der identifizierten Datenschutzrisiken

Insbesondere muss jede Partei vor der Übermittlung personenbezogener Daten an eine andere Partei, die sich außerhalb der EU bzw. des EWR befindet, prüfen, ob letztere in der Lage ist, die in den verbindlichen internen Datenschutzvorschriften vorgesehenen Garantien in der Praxis zu gewährleisten, wobei der Kontext und der Zweck der Datenübermittlung sowie die mögliche Beeinträchtigung der Grundrechte der betroffene Personen durch geltende Gesetze oder geltende Datenschutzgesetze im jeweiligen Drittland zu berücksichtigen sind. Ist dies nicht der Fall, müssen die Parteien prüfen, ob sie ergänzende technische, organisatorische oder vertragliche Maßnahmen/Kontrollen bereitstellen können, um ein den Gegebenheiten in der EU im Wesentlichen gleichwertiges Schutzniveau zu gewährleisten. Können solche Maßnahmen nicht ergriffen werden, führt die Partei die Übermittlung nicht durch. Wenn die Partei bereits personenbezogene Daten übermittelt, muss die Übermittlung ausgesetzt oder beendet werden. Sämtliche bereits übermittelten personenbezogenen Daten oder Kopien davon müssen der übermittelnden Partei vom Empfänger zurückgegeben oder vom Empfänger zerstört werden. Alle unter diesen Abschnitt fallenden Bewertungen müssen regelmäßig überprüft werden.

Die Risikobewertung umfasst die folgenden Hauptschritte:

iv. Vorabbewertung

Im Rahmen der Vorabbewertung werden die mit einer Datenverarbeitungsaktivität verbundenen Datenschutzrisiken ermittelt und jeweils als hoch, mittel oder niedrig klassifiziert. Ausgehend von den Ergebnissen der Vorabbewertung werden die weiteren Risikobewertungsschritte festgelegt.

v. Kontrollenbewertung

Im Rahmen der Kontrollenbewertung wird ausgehend von drei Ausgereiftheitsstufen ermittelt und dokumentiert, welche Maßnahmen/Kontrollen bereits implementiert wurden oder noch implementiert werden müssen, um die während der Vorabbewertung ermittelten Risiken sowie gegebenenfalls im Rahmen einer Datenschutz-Folgenabschätzung ermittelte hohe Risiken einzudämmen und die Anforderungen der verbindlichen internen Datenschutzvorschriften und der geltenden Datenschutzgesetze zu erfüllen.

vi. Bewertung der Angemessenheit von Datenschutzkontrollen

In diesem Schritt wird die Angemessenheit der implementierten oder noch zu implementierenden technischen, organisatorischen oder vertraglichen Maßnahmen beurteilt, um Datenschutzrestrisiken zu ermitteln.

vii. Risikobericht

Die identifizierten Kontrolllücken und potenziellen Restrisiken werden in einem Bericht erfasst und dokumentiert. Bevor die Datenverarbeitungsaktivität durchgeführt wird, müssen alle Lücken geschlossen, die Risiken behoben und die eindämmenden technischen und organisatorischen Maßnahmen implementiert werden.

Wenn während der Vorabbewertung ein hohes Datenschutzrisiko festgestellt wird, muss der zuständige (lokale) Datenschutzberater zusätzlich eine Datenschutz-Folgenabschätzung durchführen. Diese ist vom zuständigen Datenschutzbeauftragten abzunehmen.

8 Datenschutz-Folgenabschätzungen

Jede Partei hat vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge hat. Dabei ist der Rat des zuständigen Datenschutzbeauftragten einzuholen.

Bei der Entscheidung über die Notwendigkeit einer Datenschutz-Folgenabschätzung hat die Partei die Form der Verarbeitung, die etwaige Verwendung neuer Technologien sowie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen. Wird bei einer Datenschutz-Folgenabschätzung festgestellt, dass eine bestimmte Datenverarbeitungsaktivität ein hohes Risiko birgt, so implementiert die verantwortliche Partei vor der Verarbeitung angemessene Maßnahmen, um die entsprechenden Risiken zu mindern. Wird bei einer Datenschutz-Folgenabschätzung festgestellt, dass die Verarbeitung auch nach der Implementierung der risikomindernden Maßnahmen weiterhin ein hohes Risiko birgt, sollte vor der Verarbeitung die betroffene Aufsichtsbehörde zurate gezogen werden.

Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

i. bei systematischer, umfassender und automatisierter Verarbeitung personenbezogener Daten einschließlich Profiling und wenn die Verarbeitung als Grundlage für Entscheidungen dient, die natürliche Personen in erheblicher Weise beeinträchtigen

ii. bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

9 Rechte betroffener Personen

Jede Partei versetzt betroffene Personen in die Lage, die folgenden Rechte auszuüben.

Jede Partei informiert die Empfänger, falls eine betroffene Person eine Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung der personenbezogenen Daten verlangt, es sei denn, eine solche Unterrichtung erweist sich als unmöglich oder ist mit unverhältnismäßig hohem Aufwand verbunden. Die Parteien informieren die betroffene Person auf Aufforderung der betroffenen Person über die entsprechenden Empfänger. Alle Anträge bezüglich der vorgenannten Rechte, die eine Partei von betroffenen Personen erhält, werden gemäß den in Abschnitt 10.2 der vorliegenden verbindlichen internen Datenschutzvorschriften dargelegten Verfahren zur Beschwerdebehandlung bearbeitet.

9.1 Recht auf Zugang zu personenbezogenen Daten

Die betroffene Person hat das Recht, Zugang zu/Auskunft über die sie betreffenden personenbezogenen Daten zu verlangen sowie Informationen zum Verarbeitungszweck, zu den Kategorien personenbezogener Daten, die verarbeitet werden, zu den Empfängern der personenbezogenen Daten, zur Dauer, für die die personenbezogenen Daten aufbewahrt werden, oder zu den Kriterien für die Festlegung dieser Dauer, über das Recht, die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person zu verlangen oder gegen die Verarbeitung Widerspruch einzulegen, über das Recht, bei einer Aufsichtsbehörde Beschwerde einzulegen, sowie zur Quelle der personenbezogenen Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden. Ferner hat sie das Recht, Informationen zu verlangen hinsichtlich des Bestehens einer automatisierten Entscheidungsfindung einschließlich Profiling sowie hinsichtlich aller Übermittlungen in ein Land außerhalb der EU bzw. des EWR. Schließlich kann die betroffene Person auch eine Kopie der personenbezogenen Daten verlangen, die Gegenstand der Verarbeitung sind. (Siehe auch Abschnitt 6.2.)

9.2 Recht auf Berichtigung personenbezogener Daten

Die betroffene Person hat das Recht, die Berichtigung unrichtiger oder unvollständiger sie betreffender personenbezogener Daten zu verlangen, die von einer Partei verarbeitet werden, und unvollständige personenbezogene Daten vervollständigen zu lassen.

9.3 Recht auf Löschung personenbezogener Daten

Die betroffene Person hat das Recht, die Löschung ihrer von einer Partei verarbeiteten personenbezogenen Daten zu verlangen, vorausgesetzt dass und soweit eine der folgenden Bedingungen erfüllt ist: (I) Die personenbezogenen Daten werden im Zusammenhang mit den Zwecken, für die sie erhoben oder anderweitig verarbeitet wurden, nicht mehr benötigt, (ii) die betroffene Person widerruft die Einwilligung, welche der Verarbeitung zugrunde liegt, und es besteht keine sonstige Rechtsgrundlage für die Verarbeitung, (iii) die betroffene Person widerspricht der Verarbeitung, und es bestehen keine vorrangigen berechtigten Gründe für die Verarbeitung, oder die betroffene Person widerspricht der Verarbeitung für die Zwecke von Direktwerbung, was Profiling einschließt, soweit dieses mit Direktwerbung in Zusammenhang steht, (iv) die personenbezogenen Daten wurden unrechtmäßig verarbeitet, oder (v) die personenbezogenen Daten müssen zur Einhaltung einer rechtlichen Verpflichtung nach einem geltenden Gesetz, dem der Verantwortliche untersteht, gelöscht werden. Bestehende Datenaufbewahrungspflichten und/oder widerstreitende Interessen müssen berücksichtigt werden; es kommt Abschnitt 3.4 zur Anwendung.

9.4 Recht auf Einschränkung der Verarbeitung personenbezogener Daten

Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung der sie betreffenden personenbezogenen Daten zu verlangen, wenn (i) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird oder die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat (siehe Abschnitt 9.6 unten), und zwar für eine Dauer, die es der betreffenden Partei ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen oder zu überprüfen, ob die berechtigten Gründe der Partei gegenüber denen der betroffenen Person überwiegen, oder wenn (ii) die Verarbeitung unrechtmäßig ist oder für die verfolgten Zwecke nicht mehr erforderlich ist, die betroffene Person jedoch die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt (z. B. wenn die personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden).

9.5 Recht auf Datenübertragbarkeit und Übermittlung personenbezogener Daten

Wenn die personenbezogenen Daten von der betroffenen Person bereitgestellt wurden, wenn die Verarbeitung auf einer Einwilligung der betroffenen Person oder auf einem Vertrag mit der betroffenen Person beruht und wenn die Verarbeitung mithilfe automatisierter Verfahren erfolgt, hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten in einem gängigen und maschinenlesbaren Format zu erhalten und die personenbezogenen Daten (im Rahmen der technischen Möglichkeiten) ohne Behinderung zu übermitteln, um ähnliche Dienste eines anderen Verantwortlichen zu nutzen.

9.6 Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch einzulegen gegen eine Verarbeitung sie betreffender personenbezogener Daten, die auf berechtigten Interessen der Parteien oder Dritter oder auf öffentlichen Interessen beruht. (Dieses Recht gilt nicht, wenn die Verarbeitung der personenbezogenen Daten gesetzlich vorgeschrieben ist.) Die Verarbeitung wird eingestellt, es sei denn, die betreffende Partei kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Ferner hat die betroffene Person das Recht, Widerspruch einzulegen gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke von Direktwerbung. Dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

9.7 Recht auf Schutz vor automatisierten Entscheidungen

Betroffene Personen haben auch das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung (einschließlich Profiling) beruhenden Entscheidung einer Partei unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich

beeinträchtigen könnte. Dies gilt nicht, wenn auf die Entscheidung eine der folgenden Bedingungen zutrifft:

i. Sie ist erforderlich für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und der betreffenden Partei oder erfolgt mit ausdrücklicher Einwilligung der betroffenen Person. Voraussetzung ist, dass die betreffende Partei angemessene Maßnahmen getroffen hat, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens der Partei, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

ii. Sie ist zulässig aufgrund von geltenden Gesetzen, denen die betreffende Partei unterliegt und die angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten. Abschnitt 3.4 bleibt unberührt.

Zu diesem Zweck dürfen besondere Kategorien personenbezogener Daten nur dann verarbeitet werden, wenn entweder die betroffene Person ihre ausdrückliche Einwilligung dazu erteilt hat, oder wenn es aufgrund von geltenden Gesetzen, denen die betreffende Partei unterliegt, zulässig ist, wobei auf ein angemessenes Verhältnis zum verfolgten Ziel zu achten ist, der Wesensgehalt des Rechts auf Datenschutz gewahrt werden muss und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen sind.

10 Einhaltung der verbindlichen internen Datenschutzvorschriften

10.1 Zugang zu den verbindlichen internen Datenschutzvorschriften

Jede Partei macht die vollständigen verbindlichen internen Datenschutzvorschriften, insbesondere diejenigen Abschnitte, die Rechte betroffener Personen regeln, insbesondere Abschnitt 3.3, 3.4, 4, 6.1 – 6.8, 9.1- 9.7 und 10.1-10.4 der verbindlichen internen Datenschutzvorschriften, betroffenen Personen über das Internet auf der speziellen Fresenius-Konzern Webseite zugänglich. Die vollständigen verbindlichen internen Datenschutzvorschriften werden auch intern über die Intranet Webseiten der Fresenius-Gruppe zugänglich gemacht. Betroffene Personen können auch die vollständigen zur Veröffentlichung freigegebenen Versionen der verbindlichen internen Datenschutzvorschriften vom zuständigen Datenschutzbeauftragten sowie von jedem Mitglied der Datenschutzorganisation anfordern.

10.2 Beschwerdebehandlung im Rahmen der verbindlichen internen Datenschutzvorschriften

Jede betroffene Person kann einen Verstoß gegen die verbindlichen internen Datenschutzvorschriften anzeigen, ihre Rechte aus Abschnitt 9 der vorliegenden verbindlichen internen Datenschutzvorschriften oder jedes andere in den verbindlichen internen Datenschutzvorschriften formulierte Recht geltend machen sowie jeden beliebigen anderen Antrag an die Datenschutzorganisation stellen. Fresenius wird Prozesse implementieren, die gewährleisten, dass Beschwerden bearbeitet werden.

Eine Beschwerde ist jede Meldung eines potenziellen Verstoßes gegen die verbindlichen internen Datenschutzvorschriften, geltende Datenschutzgesetze, Beschlüsse oder Verfügungen von Aufsichtsbehörden, interne Richtlinien und Leitlinien oder freiwillige Selbstverpflichtungen mit Datenschutzbezug. Im Gegensatz dazu sind Anträge zu Rechten betroffener Personen alle Anträge betroffener Personen, die sich auf die Rechte nach Abschnitt 9 dieser verbindlichen internen Datenschutzvorschriften im Einklang mit einem Behandlungsverfahren für Anträge betroffener Personen beziehen.

Zur Übermittlung aller dieser Arten von Beschwerden stehen jeweils mehrere Kanäle zur Verfügung. Anträge können beispielsweise telefonisch oder schriftlich (z. B. per E-Mail oder Brief) übermittelt werden oder mündlich gegenüber dem zuständigen Datenschutzbeauftragten, dem zuständigen (lokalen) Datenschutzberater oder der Compliance-Hotline gestellt werden. Die entsprechenden Kontaktmöglichkeiten mit allen erforderlichen Informationen werden auf der Internetpräsenz von Fresenius sowie auf den internen Websites der Fresenius-Gruppe

veröffentlicht (https://www.fresenius.com/compliance – Hinweise auf potenzielle Compliance-Vorfälle oder https://www.fresenius-kabi.com/responsibilities/compliance).

Missbräuchlich eingereichte Beschwerden, besonders wenn sie offenkundig unbegründet oder unverhältnismäßig sind, insbesondere wegen ihres repetitiven Charakters, oder die eine Beleidigung gegen Fresenius oder einen Mitarbeiter darstellen, werden zurückgewiesen. In diesem Fall erhält die betroffene Person eine schriftliche Erklärung der Gründe der Zurückweisung und ein Einspruchsrecht.

Wird die Beschwerde als berechtigt eingestuft, ergreift die Partei eine oder mehrere angemessene Maßnahmen, um die Beschwerde mit angemessenem Aufwand zu bearbeiten und der Situation, die zu der Beschwerde Anlass gab, abzuhelfen. Die betroffene Person wird schriftlich darüber informiert, dass eine oder mehrere angemessene Maßnahmen zur Behebung der Beschwerde ergriffen werden oder ergriffen worden sind. In jedem Fall wird die betroffene Person im Einklang mit Abschnitt 10.3 über ihr Recht informiert, gerichtliche Schritte einzuleiten oder Beschwerde bei einer Aufsichtsbehörde einzulegen, wenn sie mit der Bearbeitung ihrer Beschwerde nicht zufrieden ist.

Bei Anfragen betroffener Personen bemüht sich der Datenschutzbeauftragte mit Unterstützung des (lokalen) Datenschutzberaters, der betroffenen Person wann immer möglich innerhalb eines (1) Kalendermonats ab Erhalt der Beschwerde eine ausführliche Antwort zukommen zu lassen. Sollte es unmöglich sein, innerhalb eines (1) Kalendermonats eine ausführliche Antwort zu senden, beispielsweise aufgrund der Art der Beschwerde, so informiert der zuständige Datenschutzbeauftragte die betroffene Person mit Unterstützung des (lokalen) Datenschutzberaters diesbezüglich und gibt eine Einschätzung, wann mit einer ausführlichen Antwort zu rechnen ist. Die ausführliche Antwort wird nicht später als drei (3) Monate nach Erhalt der Beschwerde gegeben.

Die Kontaktdaten des Datenschutzbeauftragten und anderer Mitglieder der Datenschutzorganisation sind auch weiter oben in Abschnitt 5 dieser verbindlichen internen Datenschutzvorschriften aufgeführt.

Die Datenschutzorganisation dokumentiert Maßnahmen betroffener Personen im Einklang mit diesem Abschnitt 10.2.

10.3 Haftung und Durchsetzung

Betroffene Personen, denen Beeinträchtigungen oder Schäden entstehen aus einer von einer Partei oder einem beauftragten Auftragsverarbeiter bzw. Unterauftragsverarbeiter durchgeführten unrechtmäßigen oder den vollziehbaren Teilen dieser verbindlichen internen Datenvorschriften gemäß Abschnitt 4 zuwiderlaufenden Verarbeitung sie betreffender personenbezogener Daten, haben das Recht, vor einem zuständigen Gericht Klage auf Durchsetzung dieser Teile der verbindlichen internen Datenschutzvorschriften sowie gegebenenfalls auf Schadenersatz zu erheben. Dies kann in dem Land geschehen, in dem die betreffende Partei ihren Sitz hat, in Bad Homburg, Deutschland, wo die FSE und die FK AG ihren Sitz haben, oder in dem Land, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Ferner kann sich die betroffene Person an Aufsichtsbehörden wenden (z. B. durch eine Beschwerde), insbesondere in dem Land, in dem sich ihr gewöhnlicher Aufenthaltsort oder ihr Arbeitsort befindet oder in dem die mutmaßliche Verletzung stattgefunden hat.

Bei nachgewiesenen Verstößen gegen die vollziehbaren Teile der verbindlichen internen Datenschutzvorschriften gemäß Abschnitt 4 durch Parteien außerhalb der EU bzw. des EWR übernimmt die FSE die Verantwortung und die Haftung für jegliche durch den Verstoß gegen die verbindlichen internen Datenschutzvorschriften entstandenen Schäden. Ferner leitet sie geeignete Maßnahmen ein, um bezüglich der Handlungen von Parteien außerhalb der EU bzw. des EWR Abhilfe zu schaffen und Schadenersatz zu leisten für alle materiellen oder immateriellen Schäden, die der betroffenen Person wegen des Verstoßes entstanden sind. Bevor Schadensersatz geleistet oder eine Erklärung gegenüber der betroffenen Person abgegeben wird, setzt die FSE die betroffene Partei unverzüglich über den geltend gemachten Anspruch in Kenntnis und gibt ihr Gelegenheit zur Erwirkung einer Schutzverfügung oder Einlegung eines anderen angemessenen Rechtsmittels. Die FSE hat das Recht, hinsichtlich mutmaßlicher Verstöße selbst eine Schutzverfügung zu erwirken oder ein anderes angemessenes Rechtsmittel einzulegen.

Kann die betroffene Person erlittene Schäden nachweisen und logisch zusammenhängend darstellen, dass die mutmaßlichen Verstöße bzw. die Schäden aufgrund des mutmaßlichen

Verstoßes gegen die verbindlichen internen Datenschutzvorschriften entstanden sind, so hat die FSE gegenüber der betroffenen Person nachzuweisen, dass die schadensverursachende Partei nicht verantwortlich war für den Verstoß gegen die verbindlichen internen Datenschutzvorschriften, der zu den Schäden geführt hat, oder dass kein solcher Verstoß vorgekommen ist. Die schadensverursachende Partei hat die FSE angemessen bei der zeitnahen Bearbeitung von Beschwerden und Anträgen zu unterstützen.

Parteien außerhalb der EU bzw. des EWR haben allen Anträgen und Verfügungen einer Aufsichtsbehörde Folge zu leisten, die bindend für die Partei wären, so als ob die Partei ihren Sitz in der EU bzw. im EWR hätte.

10.4 Kooperation mit Aufsichtsbehörden

Jede Partei muss (i) mit den zuständigen Aufsichtsbehörden zusammenarbeiten, (ii) Empfehlungen jedes Themas bezüglich der Auslegung dieser verbindlichen internen Datenschutzvorschriften umsetzen, (iii) Audits durch die zuständigen Aufsichtsbehörden zulassen. Auf Aufforderung der zuständigen Aufsichtsbehörde stellt der zuständige Datenschutzbeauftragte eine Kopie des jeweiligen Auditberichts, der im Rahmen des in Abschnitt 10.6 dargelegten Auditprogramms erstellt wurde, zur Verfügung.

10.5 Schulung

Jede Partei meldet diejenigen ihrer Mitarbeiter, die in die Verarbeitung personenbezogener Daten oder die Entwicklung von für die Verarbeitung personenbezogener Daten verwendeten Tools involviert sind, zu Schulungen über die verbindlichen internen Datenschutzvorschriften und die geltenden Datenschutzgesetze an und verpflichtet sie zur Teilnahme daran sowie zur regelmäßigen Wiederholung der Schulung. Allgemeine Schulungen müssen allen relevanten Mitarbeitern mindestens alle zwei Jahre angeboten werden. Des Weiteren werden rollenspezifische Schulungen (wie fachspezifische Informationen und Coaching oder Workshops) bereitgestellt, bei denen der konkrete Bedarf bestimmter Rollen/Personen berücksichtigt wird, beispielsweise der Bedarf von Mitgliedern der Datenschutzorganisation der FSE und der FK AG.

Die Schulung ist für relevante Mitarbeiter verpflichtend. Sobald ein Mitarbeiter zur Teilnahme an einer Schulung eingeladen wird, wird ihm ein vorab festgelegter Zeitraum für den Abschluss der Schulung mitgeteilt. Mitarbeiter, die eine Schulung bis zu einem vorgegebenen Zeitpunkt nicht absolviert haben, erhalten eine Erinnerung. Zusätzlich erhält der Vorgesetzte des Mitarbeiters eine Erinnerung, die monatlich erneut verschickt wird, bis die Schulung abgeschlossen wurde. Hat ein Mitarbeiter eine bestimmte Schulung nach zwei Erinnerungen noch nicht absolviert, kann dies (disziplinarische) Konsequenzen im Einklang mit den geltenden arbeitsrechtlichen Bestimmungen nach sich ziehen.

In den meisten Fällen werden Schulungen über eine E-Learning-Plattform durchgeführt. Allgemein enden Schulungen mit einer Validierung, welche die Festigung des Verständnisse der Inhalte unterstützt, z.B. mithilfe eines Multiple-Choice-Tests oder eines Test mit Freitextfeldern.

10.6 Audits

Die Parteien setzen ein Auditprogramm um und verpflichten sich zu dessen dauerhafter Aufrechterhaltung. Das Konzept deckt alle datenschutzrelevanten Bereiche der Parteien ab, insbesondere alle Aspekte, die unter die verbindlichen internen Datenschutzvorschriften fallen. Alle Parteien verpflichten sich zur Teilnahme an regelmäßigen Audits, in deren Rahmen die Einhaltung der verbindlichen internen Datenschutzvorschriften bewertet und getestet wird. Ferner implementieren sie angemessene und ausreichende Mechanismen zur Behebung von Verstößen gegen die verbindlichen internen Datenschutzvorschriften. Durchgeführt werden angekündigte Audits, die auf Aufforderung durch die Datenschutzorganisation oder das Management der Parteien um Ad-hoc-Audits ergänzt werden

Angekündigte Audits müssen *unter anderem* die folgenden Bereiche abdecken: (i) Datenschutz-Governance (z.B. das Ausmaß, in dem Datenschutzrichtlinien und -verfahren im Einklang mit den verbindlichen internen Datenschutzvorschriften vorhanden sind und angewendet werden etc.), (ii) Sicherheit personenbezogener Daten (z.B. vorhandene technische oder organisatorische Maßnahmen zur Gewährleistung der angemessenen Sicherheit der personenbezogenen Daten etc.), (iii) Schulungen und Bewusstsein (z.B. Bereitstellung von und Teilnahme an Datenschutzschulungen etc.), (iv) Anträge betroffener Personen bei Aufsichtsbehörden (z.B.

laufende Verfahren zur Beantwortung von Anträgen betroffener Personen sowie Kommunikation mit Aufsichtsbehörden etc.), (v) Datenübertragungen: Einhaltung der verbindlichen internen Datenschutzvorschriften insbesondere basierend auf potenziellen Beeinträchtigungen durch geltende Gesetze etc.

Die Häufigkeit und Reihenfolge angekündigter Audits wird basierend auf den Risiken, die mit den relevanten Übertragungen verbunden sind, jährlich in einem Auditplan festgelegt, wobei *unter anderem* die folgenden Aspekte berücksichtigt werden: (i) Menge der personenbezogenen Daten, (ii) Sensibilität personenbezogener Daten (einschließlich der Frage, ob besondere Kategorien personenbezogener Daten betroffen sind), (iii) Arten betroffener Personen, (iv) die kritische Bedeutung für den internen Betrieb sowie (v) potenzielle Auswirkungen auf betroffene Personen, insbesondere basierend auf durchgeführten Datenschutz-Folgenabschätzungen (siehe Abschnitt 8). Die Anzahl der innerhalb eines Jahres geprüften Parteien darf jedoch nicht unter fünf liegen.

Der Umfang von Ad-hoc-Audits wird von der Datenschutzorganisation oder dem Management der Parteien von Fall zu Fall festgelegt.

Als Ergebnis jedes Audits wird ein Auditbericht verfasst und offiziell weitergeleitet an alle Auditierten, den zuständigen Vorstand bzw. die zuständige Geschäftsleitung des kontrollierenden Unternehmens, den lokalen Datenschutzberater, den zuständigen Datenschutzbeauftragten und den Chief Compliance Officer der Parteien. Die Datenschutzorganisation führt eine Nachverfolgung aller durchgeführten Audits durch, um zu prüfen, ob vorgeschlagene Korrekturmaßnahmen angemessen umgesetzt wurden, und dokumentiert alle Ergebnisse im Auditbericht. Alle Parteien stellen den Aufsichtsbehörden die Auditberichte auf Anfrage zur Verfügung.

Audits werden entweder von den Datenschutzbeauftragten, von der internen Auditabteilung von Fresenius oder von externen Prüfern in Zusammenarbeit mit den Datenschutzbeauftragten des jeweiligen Sektors durchgeführt unter Berücksichtigung von Interessenkonflikten, indem ausgeschlossen wird, dass der Prüfer seinen eigenen Arbeitsbereich prüft.

10.7 Aktualisierung der verbindlichen internen Datenschutzvorschriften

Die Datenschutzgesetze sowie die Mittel, der Umfang und der Zweck der Datenverarbeitung im Allgemeinen entwickeln sich kontinuierlich weiter. Die Parteien werden kommende Neuerungen umgehend prüfen und entscheiden, ob Änderungen der verbindlichen internen Datenschutzvorschriften erforderlich sind. Aus diesem Grund behält sich Fresenius das Recht vor, die verbindlichen internen Datenschutzvorschriften abzuändern. Solche Änderungen umfassen ohne Einschränkung die Aufnahme neuer Parteien in die verbindlichen internen Datenschutzvorschriften oder die Streichung von Parteien aus den verbindlichen internen Datenschutzvorschriften.

Alle Parteien sowie die Aufsichtsbehörde in Hessen, Deutschland (federführende Stelle für die verbindlichen internen Datenschutzvorschriften) werden unverzüglich über alle Änderungen an den verbindlichen internen Datenschutzvorschriften informiert, die erhebliche Auswirkungen auf das durch die verbindlichen internen Datenschutzvorschriften garantierte Datenschutzniveau oder auf die verbindlichen internen Datenschutzvorschriften selbst haben. Dies schließt verwaltungstechnische Änderungen ein, soweit sie Auswirkungen auf die verbindlichen internen Datenschutzvorschriften haben. Sämtliche anderen nicht wesentlichen Änderungen an den verbindlichen internen Datenschutzvorschriften werden der Aufsichtsbehörde in Hessen, Deutschland, einmal jährlich mitgeteilt, einschließlich einer kurzen Darlegung der Gründe, welche die Änderung rechtfertigen. Die Parteien werden über solche Änderungen so schnell wie möglich in Kenntnis gesetzt, in jedem Fall spätestens zwei (2) Monate vor Inkrafttreten der Änderung oder Abwandlung der verbindlichen internen Datenschutzvorschriften. Alle Änderungen und Abwandlungen der verbindlichen internen Datenschutzvorschriften werden jährlich veröffentlicht. Um Zweifel auszuschließen: Der Aufsichtsbehörde in Hessen, Deutschland, steht es frei, diese Berichte an andere Aufsichtsbehörden weiterzugeben.

Die Datenschutzbeauftragten der FSE und der FK AG pflegen gemeinsam ein aktuelles Verzeichnis mit (i) Informationen zu allen an die verbindlichen internen Datenschutzvorschriften gebundenen Parteien und (ii) Aufzeichnungen aller Aktualisierungen der verbindlichen internen

Datenschutzvorschriften. Ferner ermöglichen sie den Aufsichtsbehörden oder betroffenen Personen auf Aufforderung Zugang zu den Informationen in diesem Verzeichnis.

11 Austritt

Wenn eine Partei aus den verbindlichen internen Datenschutzvorschriften austritt (z. B. durch Kündigung der betreffenden gruppeninternen Vereinbarung), wird die betreffende Partei entweder (i) unverzüglich jeweils alle personenbezogenen Daten an die Parteien zurücksenden, die während der Dauer, für die die verbindlichen internen Datenschutzvorschriften für die austretende Partei bindend waren, personenbezogene Daten an die Partei übermittelt haben, oder (ii) unter Einhaltung der vor Ort geltenden Datenaufbewahrungsregeln alle derartigen personenbezogenen Daten vernichten und die Vernichtung der personenbezogenen Daten gegenüber den übermittelnden Parteien schriftlich bestätigen oder (iii) bezüglich der personenbezogenen Daten andere ausreichende Garantien im Sinne von Artikel 44ff. DSGVO geben (z. B. durch Umsetzung von durch die Europäische Kommission verabschiedeten Standardvertragsklauseln). Wenn die austretende Partei keine ausreichenden Garantien bieten kann, darf die austretende Partei mit der Verarbeitung zukünftig nur in dem Umfang fortfahren, in dem eine Ausnahme gemäß Artikel 49 DSGVO zutrifft (d.h. lediglich für Zwecke, die von der jeweils geltenden Ausnahme abgedeckt sind).

12 Referenzdokumente

–

13 Änderungshistorie des Dokuments

Version	Grund und Beschreibung der Änderung	Datum
1.0	Endgültige Fassung nach Genehmigung durch den Europäischen Datenschutzausschuss	

Anhang 1: Liste der an die verbindlichen internen Datenschutzvorschriften gebundenen Parteien

[siehe separates Dokument]

Anhang 2: Arten von übermittelten personenbezogenen Daten

Die nachfolgend aufgeführten personenbezogenen Daten werden unter Einhaltung der verbindlichen internen Datenschutzvorschriften für die folgenden Zwecke übermittelt:

Personalwesen

Die folgenden personenbezogenen Daten von Managern, Mitarbeitern und Bewerbern einer Partei können zu den hier beschriebenen Zwecken an andere Parteien übermittelt werden:

Zweck	Datenkategorien
• Verwaltung des Arbeitsverhältnisses • Verwaltung/Nutzung von Mitarbeiter-IT und Mitarbeiterkommunikation • Externe Kommunikation und Website • Workflowmanagement, Leistungsmanagement, Sanktionen • Wissensmanagement, Lernmanagement • Vergütungsmanagement/Gehaltsabrechnung/Zusatzleistungen/Rentenansprüche • Personaleinsatzplanung und Ressourcenplanung • Personalbeschaffung, Karriereentwicklung und Personalbesetzung • Interne Kommunikation, Intranet • Fusionen und Akquisitionen • Compliance, behördliche Anfragen	• Identifikationsdaten und persönliche Merkmale (Name, Alter, Geschlecht, Nationalität, Ausweisnummer, Bild und Kontaktdaten) • Anstellungsbedingungen, Qualifikationen, Tätigkeitsbeschreibung • Finanzdaten (Gehalt, Versicherungsstatus, Steuern, Rentenbezüge und Zusatzleistungen) • Arbeitsplanung und Arbeitsleistung (Workflow, Projekte und Aufgaben, geleistete Arbeitsstunden, Beurteilung, Sanktionen) • Mitgliedschaft in Gewerkschaften oder Betriebsrat • Gesundheitszustand • Kommunikation und IT-Nutzung • Compliance-Untersuchungen • Information über Rechtsstreitigkeiten • Polizeiliche Führungszeugnisse (vorausgesetzt, dass sie keine Einträge haben)

Kunden

Die folgenden personenbezogenen Daten von Kunden einer Partei sowie Kundenansprechpartnern können zu den hier beschriebenen Zwecken an andere Parteien übermittelt werden:

Zweck	Datenkategorien
• Ausführung von Vereinbarungen/Fertigung, Bereitstellung und Erbringung von Produkten und Dienstleistungen/Beschwerdebehandlung • Verwaltung der Kundenbeziehung • Finanzen/Rechnungsstellung/Inkasso/Buchhaltung • Marketing/Customer-Relationship-Management und Account-Management • Fusionen und Akquisitionen • Erfüllung von Complianceanforderungen oder gesetzlichen Vorschriften, z. B. Geschäftspartner-Due-Diligence,	• Name, Funktion, Position und Kontaktdaten • Unternehmen des Kunden • Geschäftstransaktionen und Geschäftsbeziehung mit dem Kunden • Finanzdaten (Bankdaten und Rechnungsdaten) • Kommunikation und IT-Nutzung • Informationen aus öffentlichen Unterlagen, Handelsregistern und Berufsverbänden

Zweck	Datenkategorien
Sanktionslistenprüfung, Anti-Geldwäsche-Gesetze, sichere Lieferkette, Zollrecht und Exportrecht, Produktrückverfolgung, Bonitätsbewertung	

Patienten

Die folgenden personenbezogenen Daten von Patienten und medizinisch, pflegerisch oder betreuerisch tätigen Personen (z. B. Krankenpflegern) einer Partei können zu den hier beschriebenen Zwecken an andere Parteien übermittelt werden:

Zweck	Datenkategorien
• Ausführung von Vereinbarungen/Fertigung, Bereitstellung und Erbringung von Produkten und Dienstleistungen/Beschwerdebehandlung • Verwaltung der Patientenbeziehung • Marketing/Patient-Relationship-Management und Account-Management • Finanzen/Rechnungsstellung/Inkasso/Buchhaltung • Compliance und behördliche Anfragen • Fusionen und Akquisitionen • Klinische Studien, Forschung und Entwicklung • Notfallbehandlung/unerwünschte Zwischenfälle und Vigilanz	• Identifikationsdaten und persönliche Merkmale (Name, Alter, Geschlecht, Nationalität und Kontaktdaten) • Krankengeschichte und Gesundheitszustand • Behandlung und Beziehung zum Patienten • Finanzdaten (Bankdaten und Rechnungsdaten) • Kommunikation und IT-Nutzung

Zulieferer

Die folgenden personenbezogenen Daten von Zulieferern einer Partei sowie Zuliefereransprechpartnern können zu den hier beschriebenen Zwecken an andere Parteien übermittelt werden:

Zweck	Datenkategorien
• Marketing/Supplier-Relationship-Management • Verwaltung der Lieferantenbeziehung • Ausführung von Vereinbarungen/Fertigung, Bereitstellung und Erbringung von Produkten und Dienstleistungen/Beschwerdebehandlung • Finanzen/Rechnungsstellung/Buchhaltung • Fusionen und Akquisitionen • Erfüllung von Complianceanforderungen oder gesetzlichen Vorschriften, z. B. Geschäftspartner-Due-Diligence, Sanktionslistenprüfung, Anti-Geldwäsche-	• Name, Funktion, Position und Kontaktdaten • Unternehmen des Lieferanten • Geschäftstransaktionen und Geschäftsbeziehung mit dem Lieferanten • Finanzdaten (Bankdaten und Rechnungsdaten) • Kommunikation und IT-Nutzung • Informationen aus öffentlichen Unterlagen, Handelsregistern und Berufsverbänden

Zweck	Datenkategorien
Gesetze, sichere Lieferkette, Zollrecht und Exportrecht, Produktrückverfolgung, Bonitätsbewertung	

Sonstige Zwecke
Die folgenden personenbezogenen Daten von anderen natürlichen Personen (z. B. Notfallkontakten, Pressekontakten) können zu den hier beschriebenen Zwecken an andere Parteien übermittelt werden:

Zweck	Datenkategorien
• Notfallmanagement • IT • Sicherheit • Reguläre E-Mail-Verwaltung, Überwachung	• Name und Kontaktdaten • Beziehung zu Fresenius oder einer zu Fresenius gehörenden Person • Sonstige für den Zweck erforderliche Informationen