Die Verarbeitung von personenbezogenen Daten unterliegt der EU-Datenschutz-Grundverordnung (DS-GVO). Dieser Datenschutzhinweis informiert Sie[1] darüber, wie die Fresenius SE & Co. KGaA, Fresenius Digital Technology GmbH („wir" oder „Fresenius") personenbezogene Daten von Ihnen als Betroffenen („Sie") im Rahmen des Compliance Case Management verarbeiten und um welche Daten es sich dabei handelt.
Dieser Datenschutzhinweis informiert Sie zudem gemäß Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) darüber, wie Ihre personenbezogenen Daten und Informationen in Ihrer Endeinrichtung (bspw. Laptop oder Smartphone), bei der Nutzung des Hinweisgeberportals (freseniusgroup.ethicspoint.com, freseniusgroupmobile.ethicspoint.com) verarbeitet werden und um welche Daten es sich dabei handelt.
Unter "personenbezogenen Daten" verstehen wir alle Informationen über Sie als Betroffenen.
Unter "Verarbeitung" verstehen wir jeden Vorgang, der mit personenbezogenen Daten durchgeführt wird, wie z.B. Erhebung, Speicherung, Organisation, Strukturierung, Anpassung oder Änderung, Abruf, Abfrage, Nutzung, Weitergabe, Verbreitung oder anderweitige Bereitstellung, Ausrichtung oder Kombination, Einschränkung, Löschung oder Vernichtung.
Mit dieser Datenschutzinformation erläutern wir Ihnen u.a. detailliert,
- wer für die Verarbeitung Ihrer personenbezogenen Daten verantwortlich ist und an wen Sie sich wenden können, wenn Sie Fragen haben oder Beschwerden vorbringen möchten (Abschnitt 1);
- wie wir Ihre Daten erheben, welche Daten dies sind, zu welchen Zwecken wir diese personenbezogenen Daten verarbeiten, auf welche Rechtsgrundlagen wir uns hierbei stützen und wie lange wir ihre Daten speichern (Abschnitt 2);
- an wen wir Ihre Daten gegebenenfalls übermitteln (Abschnitte 3);
- wie Sie die Aktualisierung, Berichtigung oder auch die Löschung dieser Daten veranlassen und andere Rechte in Bezug auf Ihre Daten geltend machen können (Abschnitt 4) und
- geben Ihnen weitere Informationen für spezielle Situationen und Ansprechpartner (Abschnitt 5).

1. Verantwortlicher und Kontakt

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten ist für Betroffene die einen Arbeitsvertrag mit einer der folgenden Gesellschaften abgeschlossen haben bzw. in Vertragsverhandlung stehen:
- Fresenius SE & Co. KGaA, Else-Kröner-Straße 1, 61352 Bad Homburg oder
- Fresenius Digital Technology GmbH, Else-Kröner-Str. 1, 61352 Bad Homburg oder

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten ist für alle weiteren Betroffenen:
Fresenius SE & Co. KGaA, Else-Kröner-Straße 1, 61352 Bad Homburg
E-Mail: corporate-compliance@fresenius.com
Wir sind nach der DS-GVO verpflichtet, Ihnen die Kontaktdaten des Datenschutzbeauftragten zur Verfügung zu stellen. Dieser ist unter der Anschrift des Verantwortlichen z.Hd. Abteilung Datenschutz oder per E-Mail erreichbar: dataprotection@fresenius.com

2. Verarbeitung Ihrer personenbezogenen Daten

2.1 Allgemeine Verarbeitung Ihrer personenbezogenen Daten im Rahmen einer Untersuchung (Compliance Case Management)

Wir verarbeiten personenbezogene Daten die von ihnen selbst, Mitarbeitern von Fresenius Gesellschaften oder Dritten (je nach Sachverhalt von einzelnen Personen und/ oder Gesellschaften, Beschuldigten, Beteiligten oder Zeugen) bereitgestellt oder durch Nutzung unserer Systeme oder Anwendungen erhoben wurden.

Eine Untersuchung im Rahmen des Compliance Case Managements erfolgt insbesondere durch Maßnahmen zur Tatsachenermittlung, die unter anderem Folgendes umfassen können: Befragungen und Sammlung von Informationen; Analyse der Rollen und Zuständigkeiten der Betroffenen; Überprüfung von Dokumenten (z. B. Verträge, Rechnungen, Nachweise über erbrachte Dienstleistungen, Zahlungsanweisungen); Sicherstellung und Überprüfung elektronischer Daten (z. B. Analyse der auf dem Computer der Betroffenen gespeicherten Daten; Analyse von E-Mails; Daten aus SAP- oder anderen IT-Systemen, die Geschäftsprozesse abbilden bzw. unterstützen).

Wir verarbeiten Informationen, die insbesondere Sie uns selbst zur Verfügung stellen und die uns im Rahmen einer Untersuchung von anderen Mitarbeitern, anderen Fresenius-Unternehmen oder Vertragspartnern zur Verfügung gestellt werden, z.B. wenn Sie mit einem Vertragspartner E-Mails austauschen oder in einem Team mit Mitarbeitern ihrer Gesellschaft oder anderer Fresenius-Unternehmen arbeiten.
Zu diesen personenbezogenen Daten gehören insbesondere:
- Name (z. B. Vorname, Nachname, Geburtsname, Titel);
- Identifikationscode (z.B. Personalnummer, Kundennummer);
- Adress- und Kontaktdaten (z.B. Straße, Hausnummer, Postleitzahl, Wohnort, Land des Wohnsitzes, Telefonnummer, Emailadresse);
- persönliche Angaben (z.B. Geburtsdatum und Geburtsort, Familienstand, Geschlecht);
- Daten zu Anstellungsverträgen (z.B. Eintritts-/Austrittsdatum, Befristung, Urlaub, Beschäftigungsbedingungen und Arbeitsvertragsbedingungen, Pensionsberechtigung);
- Qualifikation (z.B. Bewerbungsunterlagen, Antragsunterlagen, Zertifikate, Zeugnisse, Arbeitszeugnisse, Referenzen, Patentinhaber-Informationen, Expertisen bzw. Fachkenntnisse);
- Organisatorische Angaben (z.B. Abteilung, Kostenstelle, Beschreibung der Position, Titel der Position (intern/extern), Managementkategorie, Jobcode, Berufsgruppe und Stufe, Verantwortlichkeiten und Tätigkeiten, Firmenname und Code des Arbeitgebers, Informationen zum (zu den) Vorgesetzten);
- Planungsdaten (z.B. Verfügbarkeit, Servicezeit, Vorgaben zum Zeitaufwand einer Aufgabe);
- amtlich ausgestellte Identifikatoren (z.B. Sozialversicherungsnummer, Steuernummer);

[1] Sämtliche Personenbezeichnungen in diesem Dokument gelten für alle Geschlechter gleichermaßen, auch wenn aus Gründen der besseren Lesbarkeit die männliche Form verwendet wurde.

- Unterlagen in Bezug auf Einwanderungsgesetze und Staatsbürgerschaft (z.B. nationale Identifikationsnummer, Reisepassdaten, Details zur Aufenthaltsgenehmigung oder Arbeitserlaubnis) und notwendige Informationen, um eine Aufenthalts- oder Arbeitsbewilligung zu verlängern oder zu erhalten, sowie
- Profilen in den sozialen Medien.

Wir verarbeiten Informationen, die insbesondere erhoben werden, wenn Sie eines unserer Systeme oder eine unserer Anwendungen nutzen oder sich dort anmelden.
Zu diesen personenbezogenen Daten gehören insbesondere:
- IT-Anwendungsdaten (z. B. System-Identifikatoren, Identifikator für die Einmalanmeldung, System- und Gerätepasswörter), Instant-Messaging-Konten, Videokonferenz- und andere Nachrichtenkonten, Netzwerk-ID und Infrastruktur-Informationen, IP-Adresse, Standortinformationen, WorkflowDaten (Rollen, Aktivitäten), System- und Geräteprotokolle und von Ihnen mittels unserer Unternehmenssysteme und Geräte generierte elektronische Inhalte, sowie
- Informationen in Bezug auf Qualitätsmanagement-Prozesse (z.B. Erstellung, Änderung von Qualitätsdokumenten, Datum und Uhrzeit durchgeführter Testverfahren).

Sämtliche personenbezogene und besondere personenbezogenen Daten können für die genannten Zwecke verarbeitet werden. Daher können sie ergänzend für eine Auflistung der Daten auf den ihnen vorliegenden Datenschutzhinweis für Mitarbeiter oder den über die Website www.fresenius.com veröffentlichten Datenschutzhinweis für Geschäftspartner, Besucher und Adressaten der Öffentlichkeitsarbeit zurückgreifen.

Eine Meldung im Rahmen des Compliance Case Managements kann per Website, Hotline, E-Mail, Post oder persönlich erfolgen. Eine anonyme Meldung, sowie die Einrichtung eines Postfachs zur Durchführung anonymer Gespräche kann per Website und Hotline erfolgen. Bei einer Meldung über die Hotline wird die Sprachaufnahme aufgezeichnet und schriftlich übertragen.
Das Compliance Case Management dient der Entgegennahme, Untersuchung und Beantwortung von Hinweisen auf mögliche Compliance-Verstöße bei Fresenius. Die Verarbeitung erfolgt in Übereinstimmung mit den Richtlinien von Fresenius für das Compliance Case Management Fallmanagement. Die Erforderlichkeit einer Untersuchung im Unternehmensinteresse wird dabei in einem Untersuchungsauftrag dokumentiert.
Wir verarbeiten Ihre personenbezogenen Daten ausschließlich zum Zweck der Durchführung unserer eigenen Überprüfung oder Untersuchung in dieser Angelegenheit, um einen entsprechenden Versicherungsschutz zu erhalten oder für die Zwecke der Sicherung und späteren Durchsetzung unserer Ansprüche in Bezug auf den Gegenstand der Untersuchung.

Die Berechtigung zur Verarbeitung personenbezogener Daten ergibt sich im Kontext eines Beschäftigungsverhältnisses zunächst nach Art. 6 (1) (1) (b), aus der Erforderlichkeit für die Durchführung oder Beendigung des Beschäftigungsverhältnisses, sowie Art. 9 (2) (1) (b) DS-GVO zur Ausübung von Rechten bzw. dem Nachkommen von Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes.
Für sämtliche Betroffenengruppen besteht zudem eine gesetzliche Pflicht zum Betrieb eines angemessenen internen Compliance Management Systems nach Art. 6 (1) (1) (c) DS-GVO i.V.m. § 33 (1) WpHG, § 91 (2) AktG, 43 (1) GmbHG, Art. 9 (2) (1) (f) DS-GVO und für bestimmte Beschäftigungsgeber eines Hinweisgebersystems nach Art. 6 (1) (1) (c) i.V.m. §§ 10, 12 (1) (1) HinSchG, Art. 9 (2) (1) (f) DS-GVO, § 10 (2) HinSchG.
Die Berechtigung der internen Meldestelle zur Weitergabe von Informationen über die Identität der hinweisgebenden Person ergibt sich aus Ihrer Einwilligung gemäß § 9 (3) HinSchG.

Spätestens drei Jahre nach Abschluss der internen Untersuchung werden Daten, die ausschließlich im Rahmen des Compliance Case Management verarbeitet werden, entsprechend den gesetzlichen Vorgaben gelöscht. Die Daten werden im Anschluss an die interne Untersuchung im Fall einer gerichtlichen Anspruchsdurchsetzung bzw. eines behördlichen Verfahrens für die Dauer dieses Verfahrens vorgehalten und mit dessen Beendigung gelöscht, es sei denn die Speicherung der Daten ist erforderlich für die Erhaltung von Beweismitteln für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Rahmen der gesetzlichen Verjährungsvorschriften. Nach den §§ 195ff. BGB können diese Verjährungsfristen bis zu 30 Jahre betragen, wobei die regelmäßige Verjährungsfrist drei Jahre beträgt. Zudem kann eine befristete Weiterverarbeitung erforderlich sein für die Erfüllung von Verordnungen, Gesetzen oder sonstigen Vorschriften der europäischen oder nationalen Gesetzgeber.

2.2 Zusätzliche Verarbeitung Ihrer personenbezogenen Daten auf Grund der Nutzung des elektronischen Hinweisgeberportals

2.2.1 Erfassung technischer Merkmale beim Besuch der Webseite

Wir erfassen, wie bei den meisten anderen Internetseiten auch, Daten ihres Besuchs auf unserer Website. Wenn sie unsere Webseite besuchen, verzeichnet der Webserver vorübergehend
- den Domain-Namen oder die IP-Adresse ihres Computers,
- die Dateianfrage des Clients (Dateiname und URL),
- den http-Antwort-Code,
- die Webseite von der aus sie uns besuchen,
- welchen Internetbrowser und welches Betriebssystem Sie verwenden,
- die Art ihres Gerätes,
- das Datum ihres Besuchs,
- sowie wie lange Sie sich hier aufgehalten haben.

Die Protokollierung der Daten ist für die Navigation durch die Seiten und Nutzung wesentlicher Funktionen erforderlich (§ 25 (2) (2) TDDDG, Art. 6 (1) (1) (b) DS-GVO). Eine Verwendung erfolgt zudem für Zwecke der Missbrauchserkennung und -verfolgung auf Grund der berechtigten Interessen der Datensicherheit und der Funktionsfähigkeit des Dienstes (Art. 6 (1) (1) (f) DS-GVO, § 25 (2) (2) TDDDG). Insbesondere einer Verwendung zur Abwehr von Angriffsversuchen auf unseren Webserver zur Gewährleistung einer ordnungsgemäßen Nutzung steht kein überwiegendes Interesse des Betroffenen entgegen.

Die Daten werden weder für die Erstellung von individuellen Profilen verwendet noch an Dritte weitergegeben und werden nach spätestens neunzig Tagen gelöscht.

2.2.2 Cookienutzung

Wenn Sie eine Website besuchen, kann diese Informationen über Ihren Browser abrufen oder speichern. Dies geschieht meist in Form von Cookies und ähnlichen Technologien. Das sind kleine Textdateien, die von Ihrem Webbrowser lokal auf Ihrem Computer gespeichert werden. Hierbei kann es sich um Informationen über Sie, Ihre Einstellungen oder Ihr Gerät handeln. Meist werden die Informationen verwendet, um die erwartungsgemäße Funktion der Website zu gewährleisten. Durch diese Informationen werden Sie normalerweise nicht direkt identifiziert. Die Blockierung bestimmter Arten von Cookies kann jedoch zu einer beeinträchtigten Erfahrung mit der von uns zur Verfügung gestellten Website und den von uns zur Verfügung gestellten Dienste führen.

Wir verwenden ausschließlich zwingend notwendige Cookies, damit Sie durch die Seiten navigieren und wesentliche Funktionen nutzen können. Sie ermöglichen Grundfunktionen, wie den Zugriff auf gesicherte Bereiche oder das Festlegen Ihrer Datenschutzeinstellungen. Rechtsgrundlage für diese Cookies ist § 25 (2) (2) TDDDG, Art 6 (1) (1) (b) DS-GVO. Wenn Sie diese Cookies über Ihre Browsereinstellungen blockieren, funktionieren einige oder alle dieser Funktionen möglicherweise nicht einwandfrei.

Navex.com	ASPSESSIONID*, ep, N1Secure_Incidents,	First Party	Browser Session
Navex.com	incap_ses_*, nlbi_*, reese84, x-d-token, __utcmv*	Second Party	Browser Session

Die vorgenannten Cookies werden mit Beendigung der Browser-Session automatisch gelöscht.

3. Mögliche Empfänger Ihrer personenbezogenen Daten

Um die genannten Zwecke zu erfüllen, kann es vorkommen, dass wir Ihre personenbezogenen Daten ganz oder teilweise an andere Konzerngesellschaften und/ oder Dienstleister weitergeben. Darüber hinaus können folgende Kategorien von Empfängern Ihre personenbezogenen Daten erhalten:
- Behörden, Gerichte, Parteien eines Rechtsstreits oder deren Beauftragte, denen wir auf Grund geltenden Rechts, geltender Vorschriften, rechtlicher Verfahren oder durchsetzbarer behördlicher Anordnungen Ihre personenbezogenen Daten zur Verfügung stellen müssen, z.B. Strafverfolgungsbehörden, Steuer- und Zollbehörden, Regulierungsbehörden und deren beauftragte Stellen, Finanzmarktaufsichtsbehörden, öffentliche Register;
- Wirtschaftsprüfer oder externe Berater wie Anwälte, Steuerberater, Versicherer oder Banken und
- ein anderes Unternehmen im Falle eines Eigentümerwechsels, einer Fusion, einer Akquisition oder einer Veräußerung von Vermögenswerten.

3.1 Internationale Datenübermittlung

Um den genannten Zweck zu erfüllen, kann es vorkommen, dass wir Ihre personenbezogenen Daten an Empfänger außerhalb Deutschlands übermitteln. Übermittlungen innerhalb des Europäischen Wirtschaftsraums (EWR) erfolgen stets entsprechend dem einheitlichen EU-Datenschutzniveau. Übermittlungen in Drittstaaten erfolgen stets unter Einhaltung der ergänzenden Anforderungen von Art. 44 ff. DS-GVO.
Ihre personenbezogenen Daten können in bestimmte Drittstaaten übermittelt werden, für die ein Angemessenheitsbeschluss der EU-Kommission festlegt, dass ein angemessenes Schutzniveau gemäß dem einheitlichen EU-Datenschutzniveau besteht. Die vollständige Liste dieser Länder ist hier abrufbar. (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions)
In der Regel werden bei Übermittlungen in sonstige Drittstaaten mit dem Empfänger EU-Standardvertragsklauseln abgeschlossen. Diese wurden von der EU-Kommission zur Absicherung solcher internationalen Datenübermittlungen erlassenen. Für die Übermittlung personenbezogener Daten an Konzerngesellschaften der Unternehmensbereiche Fresenius Kabi (Fresenius Kabi AG sowie die mit Ihr verbundenen Unternehmen) und Fresenius Corporate wenden wir innerhalb und außerhalb des EWR von europäischen Datenschutzbehörden gem. Art. 47 DS-GVO genehmigte verbindliche, interne Unternehmensregeln, sogenannte Binding Corporate Rules („BCR") an. Eine Kopie der SCC und der BCR kann über dataprotection@fresenius.com angefragt werden.
Letztlich können personenbezogenen Daten auf Grundlage eines Ausnahmetatbestands nach Art. 49 DS-GVO übermittelt werden.

4. Ihre Rechte

Nach der DS-GVO stehen Ihnen verschiedene Rechte zu. Sie haben das Recht, Ihre personenbezogenen Daten einzusehen (Art. 15 DS-GVO, §§ 34 ff. BDSG), falsche personenbezogene Daten zu korrigieren (Art. 16 DS-GVO), Ihre personenbezogenen Daten unter bestimmten Umständen zu löschen (Art. 17 DS-GVO, §§ 34 ff. BDSG) und unter bestimmten Voraussetzungen die Verarbeitung der Daten einzuschränken (Art. 18 DS-GVO).
Einzelfallbezogenes Widerspruchsrecht
Werden personenbezogene Daten aufgrund von Art. 6 (1) (1) (e), (f) DS-GVO verarbeitet, sowie bei einem auf diese Bestimmung gestütztem Profiling, haben Sie das Recht dieser Verarbeitung Ihrer personenbezogenen Daten aus Gründen, die sich aus Ihrer besonderen Situation ergeben, zu widersprechen (Art. 21 (1) DS-GVO).
Sie haben außerdem das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen, insbesondere in dem Mitgliedstaat Ihres gewöhnlichen Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes gegen die DS-GVO (Art. 77 DS-GVO i.V.m. § 19 BDSG). Die für Fresenius SE & Co. KGaA und Fresenius Digital Technology GmbH zuständige Datenschutzbehörde ist „Der Hessische Beauftragte für Datenschutz und Informationsfreiheit", Postfach 3163, 65021 Wiesbaden.
Das Beschwerderecht besteht unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs.

5. Weitere Informationen für spezielle Situationen und Ansprechpartner

Wir können Ihre personenbezogenen Daten in verschiedenen anderen Zusammenhängen verarbeiten, z.B. wenn Sie unsere Website www.fresenius.com besuchen. Für die Verarbeitung Ihrer personenbezogenen Daten in diesen Situationen beachten Sie bitte die jeweils spezifischen Informationen.
Wenn Sie Fragen zum Datenschutz bei Fresenius haben, wenden Sie sich bitte an dataprotection@fresenius.com.