



Erstellt: CF/D. Feiler	Erstell. Datum: 19.10.2020	Geändert am: 27.09.2022	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum: 27.09.2022
---------------------------	-------------------------------	----------------------------	----------	-----------------	--------------	---------------------------

Unsere Datenschutzrichtlinie

Liebe Mitarbeiterinnen, liebe Mitarbeiter,

als Gesundheitsdienstleister verarbeiten wir hochsensible (besonders schützenswerte) Daten unserer Kunden/Patienten. Mit zunehmendem Einsatz der Informationstechnologie (IT) und des elektronischen Datenaustausches, ist es daher besonders wichtig verantwortungsvoll und sorgsam mit den Daten unserer Patienten, Mitarbeiter und Geschäftspartner umzugehen – auch zur Erfüllung der geltenden gesetzlichen Vorgaben der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) sowie weiteren geltenden Gesetzen und Verordnungen.

Für uns gilt der Grundsatz: Wo Daten gespeichert und gesendet werden, muss ein hohes Maß an Datenschutz und Datensicherheit gewährleistet sein. Dies gilt für Daten unserer Patienten, Geschäftspartner (Lieferanten, Zuweiser) genauso wie für unsere Mitarbeiterdaten.

Unser Anspruch ist es, dass das **Radiologie Zentrum Neu-Ulm** nicht nur für eine exzellente medizinische Versorgung steht, sondern auch Standards beim Datenschutz setzt. Deshalb sehen wir es als unsere Pflicht an, als regional und überregional agierende Gesundheitsdienstleister den gesetzlichen Anforderungen zu entsprechen, die mit der Erhebung und Verarbeitung personenbezogener Daten verbunden sind. Oberste Priorität hat für uns, einen einheitlichen und gültigen Standard beim Umgang mit personenbezogenen Daten sicherzustellen.

In unserer Richtlinie zum Datenschutz haben wir strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von Patienten, Mitarbeitern und Geschäftspartnern geregelt. Diese entsprechen den Anforderungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) und stellt die Einhaltung der Prinzipien der in Deutschland geltenden Gesetzgebung sicher.

Als Maßstab haben wir die auf folgenden Seiten genannten Datenschutzgrundsätze festgelegt – darunter **Transparenz, Datensparsamkeit** und **Datensicherheit**.

Unsere Führungskräfte und Mitarbeiter sind verpflichtet, diese Richtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren. Der Datenschutz-Beauftragte trägt dafür Sorge, dass im **Radiologie Zentrum Neu-Ulm** die gesetzlichen Regelungen und Prinzipien zum Datenschutz in allen ihren Standorten beachtet werden. Für Rückfragen steht Ihnen unserer **Datenschutz-Beauftragter Herr Dennis Feiler** gerne zur Verfügung.

Dennis Feiler, c/o DFC-SYSTEMS GmbH, Einsteinring 28, 85609 Aschheim b. München. Telefon 089 461487-0, datenschutz@dfcsystems.de

I. Ziel der Datenschutzrichtlinie

Das **Radiologie Zentrum Neu-Ulm** verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung der geltenden Datenschutzrechte. Diese Datenschutzrichtlinie gilt für alle Mitarbeiter des **Radiologie Zentrum Neu-Ulm** und beruht auf den geltenden europäischen- und deutschen Richtlinien und



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feller	19.10.2020	27.09.2022				27.09.2022

Gesetzen. Sie gewährleistet das von der Europäischen Datenschutzrichtlinie und den nationalen Gesetzen verlangte angemessene Datenschutzniveau.

II. Geltungsbereich und Änderung der Datenschutzrichtlinie

Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. Anonymisierte Daten, z.B. für statistische Auswertungen oder Forschung, unterliegen nicht dieser Datenschutzrichtlinie. Die Mitarbeiter sind nicht berechtigt, von dieser Datenschutzrichtlinie abweichende Regelungen zu treffen.

III. Geltung staatlichen Rechts

Diese Datenschutzrichtlinie ergänzt die gesetzlichen Verpflichtungen der europäischen und deutschen Gesetzgebung und Verordnungen zum Datenschutz. Das jeweilige europäische und deutsche Recht geht vor, wenn es Abweichungen von dieser Datenschutzrichtlinie erfordert oder weitergehende Anforderungen stellt. Die Inhalte dieser Datenschutzrichtlinie sind auch dann zu beachten, wenn es kein entsprechendes staatliches Recht gibt. Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen müssen beachtet werden. Jeder Standort ist für die Einhaltung dieser Datenschutzrichtlinie und der gesetzlichen Verpflichtungen verantwortlich.

IV. Prinzipien für die Verarbeitung personenbezogener Daten

1. Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

2. Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden oder den gesetzlichen Anforderungen entsprechen. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

3. Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- » Die Identität der verantwortlichen Stelle
- » Den Zweck der Datenverarbeitung
- » Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden



Erstellt:
CF/D. Feller

Erstell. Datum:
19.10.2020

Geändert am:
27.09.2022

Geprüft:

Datum d. Prüf.:

Freigegeben:

Akt. Datum:
27.09.2022

Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden.

Personenbezogene Daten dürfen nicht auf Vorrat für potenzielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist rechtlich vorgeschrieben oder erlaubt.

5. Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

6. Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht Zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

7. Vertraulichkeit und Datensicherheit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

V. Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll:

1. Patientendaten

1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des Betroffenen dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Patienten, sofern dies im Zusammenhang mit dem Vertragszweck steht.



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feller	19.10.2020	27.09.2022				27.09.2022

1.2 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene entsprechend informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen.

1.3 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn rechtliche Vorschriften (z.B. SGB, MBO-Ä, BGB, etc.) die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

1.4 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des **Radiologie Zentrum Neu-Ulm | Günzburg** erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen).

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

1.5 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

1.6 Nutzerdaten und Internet

Wenn auf Webseiten personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den



Erstellt:
CF/D. Feller

Erstell. Datum:
19.10.2020

Geändert am:
27.09.2022

Geprüft:

Datum d. Prüf.:

Freigegeben:

Akt. Datum:
27.09.2022

Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out). Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

2. Mitarbeiterdaten

2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für

einen späteren Auswahlprozess eingewilligt. Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen. Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

2.3 Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feller	19.10.2020	27.09.2022				27.09.2022

angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene jedoch informiert werden.

2.4 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der **Radiologie Zentrum Neu-Ulm** erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. bei der Neu- oder Reorganisation von Unternehmensbereichen) begründet. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen.

Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen. Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechnete Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

2.5 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein.

Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortlichen Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.



Erstellt:
CF/D. Feller

Erstell. Datum:
19.10.2020

Geändert am:
27.09.2022

Geprüft:

Datum d. Prüf.:

Freigegeben:

Akt. Datum:
27.09.2022

2.6 Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein. Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

2.7 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden. Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt.

Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das Unternehmens-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Unternehmens erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Konzernregelungen.

VI. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der **Radiologie Zentrum Neu-Ulm** oder an Empfänger innerhalb der **Radiologie Zentrum Neu-Ulm** unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt V.. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

VII. Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feller	19.10.2020	27.09.2022				27.09.2022

wird (z.B. IT-Service Tätigkeiten durch Fernwartung oder vor Ort). In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss deren Umsetzung sicherstellen:

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
3. Die vom Datenschutzbeauftragten bereitgestellten Vertragsstandards müssen beachtet werden. Durch den Auftragnehmer bereitgestellte Vertragsstandards dürfen erst nach Prüfung durch den Datenschutzbeauftragten verwendet werden.
4. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.
5. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:
 - a. Vereinbarung der EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.
 - b. Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus.
 - c. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

VIII. Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.



Erstellt:
CF/D. Feller

Erstell. Datum:
19.10.2020

Geändert am:
27.09.2022

Geprüft:

Datum d. Prüf.:

Freigegeben:

Akt. Datum:
27.09.2022

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind.
2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
4. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

IX. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern der **Radiologie Zentrum Neu-Ulm** untersagt.

Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten. Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

Vorgesetzte müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

X. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des Informationssicherheitsmanagements des Unternehmens und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feiler	19.10.2020	27.09.2022				27.09.2022

XI. Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem. Die Unternehmensleitung ist über wesentliche Ergebnisse zu informieren. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

XII. Datenschutzvorfälle

Jeder Mitarbeiter soll dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle/Datenschutzpannen) melden. Die für den Fachbereich verantwortliche Führungskraft ist verantwortlich, den Datenschutzbeauftragten umgehend über Datenschutzvorfälle zu unterrichten. In Fällen von:

- » unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- » unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder
- » bei Verlust personenbezogener Daten,

damit nach staatlichem Recht bestehende Meldepflichten (**innerhalb nach 72h nach Bekanntwerden des Datenschutzvorfalles**) von Datenschutzvorfällen erfüllt werden können.

XIII. Verantwortlichkeiten und Sanktionen

Die Gesellschafter, Geschäftsführung, Fachbereichsleiter sind verantwortlich für die Datenverarbeitung im Unternehmen bzw. in ihrem Verantwortungsbereich. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. Meldepflichten). Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter (IT-Fachbereich, IT-Personal). Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.

Der Datenschutzbeauftragte ist vor Ort Ansprechpartner für den Datenschutz. Er kann Kontrollen durchführen und hat die Mitarbeiter mit den Inhalten der Datenschutzrichtlinien vertraut zu machen.

Die jeweiligen Gesellschafter, Geschäftsführung, Fachbereichsleiter sind verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen den Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren.

Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten.



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feiler	19.10.2020	27.09.2022				27.09.2022

Die Verantwortlichen (Gesellschafter, Geschäftsführung, Fachbereichsleiter) müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in Deutschland auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

Der Datenschutz-Beauftragte

Der Datenschutzbeauftragte als fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Der Datenschutzbeauftragte wird durch die Geschäftsführung bestellt. Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt. Anfragen von Aufsichtsbehörden sind immer an den Datenschutzbeauftragten zur Kenntnis zu bringen. Der Datenschutzbeauftragte und seine Mitarbeiter können wie folgt erreicht werden:

Herr Dennis Feiler

dennis.feiler@dfcsystems.de

Telefon 089 461487-0

Neu-Ulm , August 2020

XV. Definitionen

Ein angemessenes Datenschutzniveau von Drittstaaten wird von der EU-Kommission dann anerkannt, wenn der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU-Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schließt die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Landesregeln und Sicherheitsmaßnahmen ein.

Anonymisiert sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein.

Betroffener im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.



Erstellt:	Erstell. Datum:	Geändert am:	Geprüft:	Datum d. Prüf.:	Freigegeben:	Akt. Datum:
CF/D. Feiler	19.10.2020	27.09.2022				27.09.2022

Datenschutzvorfälle sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Mitarbeiter beziehen.

Dritter ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle.

Auftragsdatenverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

Drittstaaten im Sinne der Datenschutzrichtlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU-Kommission als angemessen anerkannt worden ist.

Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

Erforderlich ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.

Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.

Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

Verarbeitung personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

Verantwortliche Stelle sind die Geschäftsführung und Gesellschafter.