KLINIKUM
WOLFSBURG

Datenschutzrichtlinie

gemäß
EU-Datenschutzgrundverordnung (DSGVO)

WOLFSBURG

1. Einleitung 3
1.1 Allgemeine Anforderungen 3
1.2 Sicherheitsziele 3
2. Zielsetzung dieser Datenschutzrichtlinie 4
3. Geltungsbereich 4
4. Datenschutzorganisation/ Lenkung 4
4.1. Direktorium 5
4.2. Leitungspersonen 5
4.3. Datenschutzbeauftragter 5
4.4. Datenschutzteam 6
4.5. Datenschutzkoordinatoren 6
4.6. Arbeitskreis Datenschutzkoordinatoren 7
5. Datenschutzgrundsätze 7
5.1. Grundsätzliche Verantwortlichkeit 7
5.1.1. Fachbereichsverantwortung 8
5.1.2. Persönliche Verantwortung 8
5.2. Grundsätze der Verarbeitung personenbezogener Daten 8
5.2.1. Rechtmäßige Verarbeitung 8
5.2.2. Zweckbindung 9
5.2.3. Datenminimierung 9
5.2.4. Richtigkeit 9
5.2.5. Speicherbegrenzung 9
5.2.6. Wahrung von Integrität und Vertraulichkeit 10
5.3. Informationspflicht gegenüber dem Betroffenen 10
5.4. Verarbeitung besonderer personenbezogener Daten 10
5.5. Schadensstufen im Datenschutz 11
5.6. Sicherheit der Datenverarbeitung 12
5.6.1. Umgang mit personenbezogenen Daten 12
5.6.2. Risikoanalyse 12
5.6.3. Sicherheitskonzept 12
5.6.4. Verarbeitungsgestaltung 12
5.6.5. Datenschutzfolgeabschätzung 13
5.7. Transparenz und Dokumentation der Datenverarbeitung 14
5.8. Schutzrechte der Betroffenen 14
5.9. Umgang mit Datenschutzpannen 14
5.10. Verpflichtung, Schulung und Sensibilisierung 15
5.11. Auftragsverarbeitung 16

5.12. Sanktion bei Verstößen und Zuwiderhandlungen 16
5.13. Rechenschafts- und Dokumentationspflicht....16
6. Datenschutzmanagementsystem 17
6.1. Schulung und Sensibilisierung der Beschäftigten....17
6.2. Überprüfung und Auditierung....17
6.3. Transparenz und Dokumentation der Datenverarbeitung....18
6.4. Bearbeitung von Datenschutzanfragen....18
6.5. Bearbeitung von Datenschutzvorfällen....18
6.6. Auftragsverarbeitung durch Dienstleister 18
6.7. Risikobetrachtung und Folgenabschätzung 18
6.8. Wirksamkeit des DSMS und kontinuierliche Verbesserung....19
7. Inkrafttreten....19
8. Dokumentenhistorie 19
9. Anlage 1 Besondere Kategorien personenbezogener Daten....20
10. Anlage 2 Ergänzende Regelungen 22

1. Einleitung

1.1 Allgemeine Anforderungen

Der zuverlässige und gesetzeskonforme Einsatz von IT-Systemen und IT-gestützten Anwendungen sowie die damit verarbeiteten und gespeicherten Informationen und personenbezogenen Daten von Patienten, Beschäftigten, Kunden, Partnern, Leistungserbringern und Lieferanten sind von grundlegender Bedeutung für den Erfolg des Klinikum Wolfsburg (nachfolgend auch Klinikum genannt). Neben den gestiegenen Erwartungen der Patienten und Mitarbeiter, deren Daten durch uns verarbeitet werden, hinsichtlich eines sicheren Umganges und Schutzes ihrer Daten sind auch immer strengere gesetzliche Schutzanforderungen bezüglich der Verarbeitung von Daten zu beachten. Eine unzulässige Verarbeitung, eine Manipulation/ Verfälschung, der Verlust oder das unbeabsichtigte Öffentlichen werden von schutzbedürftigen/ personenbezogenen Daten kann für das Klinikum zu zivilrechtlichen, strafrechtlichen und finanziellen Konsequenzen führen.
Die folgenden Grundsätze beschreiben die Zielrichtung der Sicherheitspolitik unseres Unternehmens und legen die Sicherheitsmaßnahmen, die jeder Einzelne zu beachten hat, fest.

1.2 Sicherheitsziele

Neben einer verantwortungsvollen und gesetzeskonformen Datenverarbeitung und dem daraus resultierenden Vertrauen von Patienten, Lieferanten sowie Beschäftigten in unser Unternehmen ist auch der Schutz der Vermögenswerte ein wichtiges Sicherheitsziel.
Unsere wirtschaftliche Leistungsfähigkeit ist davon abhängig, dass insbesondere die Belastbarkeit, Integrität, Verfügbarkeit und Vertraulichkeit unserer Systeme, Informationen und Daten gewahrt bleiben und unsere IT-Systeme/ –Anwendungen, technischen/ organisatorischen Prozesse und unsere Beschäftigten, Partner, Leistungserbringer und Lieferanten zuverlässig und regelkonform arbeiten.

Die Einhaltung und Umsetzung der Sicherheitsziele sind ein wichtiger Bestandteil unserer Geschäftspolitik.

Innerhalb des Klinikums sind folgende Sicherheitsziele zu erreichen:

- Die Systeme und internen Geschäftsprozesse haben eine hohe Verlässlichkeit, dazu gehört die Belastbarkeit, Verfügbarkeit und die Integrität der IT-Systeme/ -Anwendungen und Daten sowie eine ausreichende Vertraulichkeit.
- Auftretende Fehler sind schnell zu erkennen; die Geschäftsprozesse sind so zu gestalten, dass Fehler vermieden werden.
- Für Geschäftsprozesse mit hohem Risiko werden nur minimale Ausfallzeiten toleriert.
- In Technik, in Arbeitsprozesse und in Informationen investiertes Wissen und Werte werden geschützt und bleiben erhalten.
- Gesetzliche Vorgaben und Anforderungen werden eingehalten.

2. Zielsetzung dieser Datenschutzrichtlinie

Die vorliegende Datenschutzrichtlinie (nachfolgend auch Richtlinie genannt) beschreibt die für das Klinikum geltenden Datenschutzgrundsätze und legt die zum Schutz personenbezogener Daten umgesetzten Prinzipien und Ziele, ihren Aufbau und ihre Überwachung fest.
Diese Richtlinie regelt somit die datenschutzkonforme Informationsverarbeitung und die insoweit beim Klinikum bestehenden Verantwortlichkeiten. Alle Beschäftigten sind zur Einhaltung der Datenschutzanforderungen verpflichtet.
Die Grundsätze stimmen mit der EU-Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) sowie dem geltenden Branchenstandard für Informationssicherheit überein.
Diese Grundsätze werden zur Zielerreichung durch weitere zusätzliche Dokumente (Methoden, Verfahren, Praxisanweisungen, Sensibilisierungsmaßnahmen etc.) ergänzt, verstärkt und konkretisiert.

3. Geltungsbereich

Diese Datenschutzrichtlinie gilt für alle Beschäftigten des Klinikums sowie für alle in dessen Auftrag tätigen Kooperationspartner, Auftragnehmer, Leistungserbringer und Lieferanten.

Sie gilt insbesondere für:

- die Personen oder Abteilungen, die über den Einsatz/die Bereitstellung eines Anwendungssystems entscheiden (insbesondere die IT-Abteilung),
- die Personen oder Abteilungen, die über die Nutzung des Systems für ihre Aufgaben entscheiden (d. h. alle administrativen Bereiche und Fachabteilungen),
- alle Benutzer, die die zur Verfügung gestellten Systeme und Anwendungen für die Erledigung ihrer betrieblichen Aufgaben nutzen.

Beschäftigte im Sinne dieser Richtlinie sind alle Arbeitnehmerinnen und Arbeitnehmer, Praktikantinnen und Praktikanten und Auszubildenden sowie Beamtinnen und Beamten.

4. Datenschutzorganisation/ Lenkung

Nachfolgend wird die betriebliche Organisation des Datenschutzes im Klinikum und die Verantwortlichkeit der beteiligten Funktionsträger beschrieben.

4.1. Direktorium

Die strategische Verantwortung für diese Datenschutzrichtlinie liegt beim Direktorium des Klinikums.
Dieses hat:

- die betriebliche Umsetzung der Richtlinie an die jeweiligen Chefärzte/ Abteilungsleitungen, Pflegedirektion, Bereichsverantwortliche
- die konzeptionelle Weiterentwicklung der Richtlinie an den Datenschutzbeauftragten sowie
- die Überwachung der Einhaltung der mit der Richtlinie festgelegten Grundsätze an die Datenschutzkoordinatoren und den Datenschutzbeauftragten

delegiert.

Das Direktorium ist über alle Probleme bei der Umsetzung der Richtlinie zu informieren.

4.2. Leitungspersonen

Die Chefärzte, Abteilungsleiter, Pflegedirektion und Bereichsverantwortliche sind als Leitungspersonen für die Einhaltung der Datenschutzgrundsätze und den Schutz der personenbezogenen Daten innerhalb ihres Verantwortungsbereiches zuständig. Sie haben die Umsetzung der mit dieser Richtlinie festgelegten Maßnahmen zu gewährleisten.
Zu ihrer/ seiner Unterstützung bei der Umsetzung von erforderlichen Maßnahmen benennt jede Leitungsperson mindestens eine/n Mitarbeiter*in zum Datenschutzkoordinator für ihre/ seinen Verantwortungsbereich. Soweit die Leitungsperson keinen Datenschutzkoordinator benennt, obliegt ihr/ ihm selbst die Aufgabe der operativen Umsetzung der Datenschutzgrundsätze und sie/ er ist zugleich Hauptansprechpartner des DSB.
In Zweifelsfällen und bei Beratungs-/ Unterstützungsbedarf wendet sich die Leitungsperson vor Beginn einer geplanten/ beabsichtigten Datenverarbeitung zur Abstimmung an den Datenschutzbeauftragten.

4.3. Datenschutzbeauftragter

Das Klinikum hat gemäß Art. 37 DSGVO einen betrieblichen Datenschutzbeauftragten (DSB) und einen Abwesenheitsvertreter bestellt. Der Datenschutzbeauftragte ist per mail über datenschutzbeauftragter@klinikum.wolfsburg.de erreichbar.
Der DSB nimmt die ihm nach Art. 38 DSGVO und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.

Der DSB unterrichtet und berät das Direktorium sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien und Verfahren des Klinikums für den Schutz personenbezogener Daten einschließlich der Sensibilisierung und Schulung der Mitarbeiter.
Der DSB hat insbesondere die folgenden Aufgaben:

- die Richtlinie im erforderlichen Umfang weiterzuentwickeln,
- auf die Umsetzung dieser Richtlinie durch die Leitungspersonen und alle Beschäftigten hinzuwirken,
- die Koordination von erforderlichen technischen / organisatorischen Maßnahmen mit den zuständigen Leitungspersonen und
- gemeinsam mit den Datenschutzkoordinatoren die Einhaltung und Wirksamkeit der Regelung der Richtlinie und mitgeltenden Dokumenten zu überwachen.

Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl vom Direktorium als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt. Im Falle risikoreicher Datenverarbeitungen unterstützt der DSB das Klinikum beratend bei der Abschätzung des Risikos.
Der DSB berichtet unmittelbar dem Direktorium. Er berichtet jährlich in einem Tätigkeitsbericht dem Direktorium über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel. Soweit der Bericht die Verarbeitung von Personaldaten oder Fragen der betrieblichen Organisation betrifft, wird er auch dem Personalrat zugänglich gemacht.
Alle Beschäftigten können sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den DSB wenden. Dieser wahrt auf Wunsch absolute Vertraulichkeit.

4.4. Datenschutzteam

Das Klinikum Wolfsburg hat zur effizienten Bearbeitung von Datenschutzthemen ein Datenschutzteam eingesetzt. Die Zusammensetzung des Datenschutzteams ist in der Leitlinie zur Informationssicherheit beschrieben. Das Team ist ein dauerhaft eingerichtetes Gremium, das die Koordination von Datenschutzaufgaben innerhalb des Klinikums zwischen allen Beteiligten sicherstellt.

Die wesentlichen Aufgaben des Datenschutzteams sind insbesondere:

- die Beratung zu aus dem Haus gestellten Anfragen,
- Formulierung von verbindlichen Handlungsvorgaben und Verhaltensempfehlungen
- Unterstützung bei der datenschutzkonformen Anpassung von Dokumenten
- Umsetzung der Transparenz- und Informationspflichten nach Art. 12 ff DSGVO
- Führung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO
- Bearbeitung von Anfragen zur Ausübung der Betroffenenrechte nach Art. 7, 15 – 21 DSGVO
- Prüfung und Bearbeitung von Datenschutzvorfällen sowie deren Meldung an die Datenschutzaufsichtsbehörde gemäß Art. 33 DSGVO. Soweit erforderlich auch Information der Betroffenen nach Art. 34 DSGVO
- Führung der Übersicht der Auftragsverarbeiter sowie deren erbrachten Verarbeitungstätigkeiten

4.5. Datenschutzkoordinatoren

Die Datenschutzkoordinatoren (DSK) unterstützen das Leitungspersonal bei der Einhaltung und Umsetzung der Datenschutzgrundsätze innerhalb der Abteilung/ Bereiche. Zur Erledigung ihrer Aufgaben müssen die DSK das notwendige Fachwissen und die erforderlichen Zeitressourcen erhalten. Der DSK informiert das Datenschutzteam oder den DSB über vor Ort aufgetretene Datenschutzfragen und stimmt sich soweit erforderlich mit diesen über geeignete Maßnahmen ab. Er erhebt die Angaben über in seinem Zuständigkeitsbereich gesondert eingesetzte Verfahren (Abteilungslösungen) und gibt die Meldung an das DS-Team oder den DSB weiter.

Die DSK haben insbesondere die Aufgabe:

- gemeinsam mit dem Datenschutzbeauftragten die Einhaltung und Wirksamkeit der Regelung der Richtlinie zu überwachen,
- als Ansprechpartner für die Beschäftigten ihrer Abteilung/ ihres Bereiches zu fungieren und
- datenschutzrelevante Fragestellungen ihrer Abteilung / ihres Bereiches mit dem Datenschutzteam und dem Datenschutzbeauftragten abzustimmen.

4.6. Arbeitskreis Datenschutzkoordinatoren

Der Arbeitskreis Datenschutzkoordinatoren dient der Klärung bereichsübergreifender Datenschutzfragestellungen. Unter der Leitung des DSB hält der Arbeitskreis mindestens vierteljährliche Arbeitstreffen aller Datenschutzkoordinatoren ab.
Der Arbeitskreis:

- berät über bereichsübergreifende Datenschutzmaßnahmen und legt diese dem Direktorium zur Genehmigung vor und
- wirkt an der Umsetzung des Datenschutzmanagementsystems (DSMS) mit, das hauptsächlich auf die Einhaltung dieser Datenschutzrichtlinie abzielt.

Einmal jährlich berichtet der Arbeitskreis dem Direktorium über seine Tätigkeit, insbesondere über die Prüfung der Umsetzung dieser Richtlinie.

5. Datenschutzgrundsätze

Der Schutz personenbezogener Daten ist dem Klinikum Wolfsburg ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Patienten, Beschäftigten, Auftragnehmer, Partner, Leistungserbringer und Lieferanten in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

Dazu sind die folgenden zusammengefassten Grundsätze zu beachten:

- Personenbezogene Daten dürfen nur in rechtlich zulässiger Form beschafft und verarbeitet werden.
- Die IT-Hard- und Software sowie alle erhobenen personenbezogenen Daten sind ausschließlich für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust, Manipulation und Zerstörung zu sichern. Eine Nutzung für private Zwecke ist grundsätzlich verboten, Ausnahmen regelt die ARDV-IT.
- Jeder Beschäftigte ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie und den daraus abgeleiteten bzw. mitgeltenden Regelungsdokumenten verantwortlich. Die Einhaltung der Regelungen ist Dienstaufgabe.
- Die für die Verarbeitungen und die eingesetzte IT-Hard- und Software Verantwortlichen (Chefärzte und Abteilungsleiter, Bereichsverantwortliche) stellen sicher, dass ihre Mitarbeiter (Benutzer) über diese Richtlinie sowie daraus abgeleitete bzw. mitgeltenden Regelungsdokumente informiert werden; das gilt auch für temporär Beschäftigte (z. B. Aushilfen, Praktikanten etc.).
- Der Datenschutzbeauftragte berät bei der Umsetzung der gesetzlichen und betrieblichen Datenschutzanforderungen aus der Datenschutzrichtlinie sowie den abgeleiteten und mitgeltenden Regelungsdokumenten und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSB gegenüber auskunftspflichtig.

Nachfolgend werden die oben genannten Grundsätze sowie weitergehende datenschutzrelevante Aspekte vertiefend dargestellt.

5.1. Grundsätzliche Verantwortlichkeit

Grundsätzlich liegt die Datenschutzverantwortung für die Verarbeitung personenbezogener Daten beim Direktorium des Klinikums.

Bereits bei der Projektplanung sowie vor dem tatsächlichen Beginn einer Verarbeitungstätigkeit oder einer beabsichtigten Datenverarbeitung sowie während der Verarbeitung bzw. bei einer Änderung der Verarbeitungsbedingungen sind die im folgenden dargestellten Grundsätze zu beachten.

5.1.1. Fachbereichsverantwortung

Jeder Fachbereich/Klinik/ Abteilung ist für jede von ihm selbst oder einem ihn unterstützenden Auftragsverarbeiter durchgeführte Verarbeitungstätigkeit bzw. Datenverarbeitung verantwortlich. Die Leitungsperson hat für die geplante Verarbeitungstätigkeit bzw. Datenverarbeitung die Beachtung der Datenschutzrichtlinie und der einschlägigen Datenschutzgesetze zu gewährleisten.
Vor Beginn einer neuen Verarbeitungstätigkeit oder der Installation einer neuen oder veränderten Anwendung zur Verarbeitung personenbezogener Daten muss der verantwortliche Fachbereich durch den DSK die Verarbeitung gemäß Art. 30 DSGVO dokumentieren und den DSB informieren, damit vor Beginn der Verarbeitung die erforderliche Überprüfung bezüglich Zulässigkeit und Sicherheit der Verarbeitung erfolgen kann.

Auftragsverarbeiter und sonstige Dienstleister, die im Namen des Klinikums Leistungen erbringen, sind durch den beauftragenden Fachbereich über die Grundsätze dieser Richtlinie bezüglich der von ihnen eingesehenen und verarbeiteten personenbezogenen Daten in Kenntnis zu setzen und zu deren Einhaltung zu verpflichten.

5.1.2. Persönliche Verantwortung

Innerhalb ihres Aufgabenbereiches sind alle vorübergehend und dauerhaft Beschäftigten für den Schutz und die rechtmäßige Verwendung der von ihnen eingesehenen und verarbeiteten personenbezogenen Daten verantwortlich.
Bei der Leitung von Projekten mit Verarbeitung personenbezogener Daten handeln der Projektleiter im Namen des oder der betroffenen Fachbereiche. Die Projektleitung muss die Einhaltung des Datenschutzes während der gesamten Projektlaufzeit gewährleisten.

5.2. Grundsätze der Verarbeitung personenbezogener Daten

Die Leitungspersonen sind für die Einhaltung und den Nachweis der Verarbeitungsgrundsätze verantwortlich. Auf Anforderung muss dieser Nachweis im Sinne der sogenannten Rechenschaftspflicht gegenüber der zuständigen Datenschutzaufsichtsbehörde (Landesbeauftragte(r) für den Datenschutz) geführt werden.

5.2.1. Rechtmäßige Verarbeitung

Personenbezogene Daten sind auf rechtmäßige Weise durch faires rechtlich zulässiges Handeln und in einer für die betroffene Person nachvollziehbaren Weise zu verarbeitet („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz).
Jede Verarbeitung von personenbezogenen Daten bedarf einer Rechtsgrundlage. Ohne gültige Rechtsgrundlage stellt eine Datenverarbeitung einen bußgeldbewährten Datenschutzverstoß dar.
Die Zulässigkeit einer Datenverarbeitung ergibt sich aus:

- einer schriftlichen Einwilligung der Person, deren Daten verarbeitet werden sollen,
- dem Abschluss eines Vertrages, zu dessen Erfüllung die Datenverarbeitung notwendig ist,
- gesetzlichen Vorgaben/ Anforderungen, denen das Klinikum unterliegt, z. B. gesetzliche Meldepflichten etc.,

- einem berechtigten Interesse des Klinikums, das schutzwürdige Belange der betroffenen Person überwiegt – Achtung: Hier ist zwingend eine Abstimmung mit dem Datenschutzbeauftragten vor Beginn der Datenverarbeitung durchzuführen.
- ggf. weiteren Anspruchsgrundlagen, die gemeinsam mit dem DSB zu überprüfen sind. – Bitte sprechen Sie im Bedarfsfalle den DSB hierzu an.

Personenbezogene Daten dürfen innerhalb des Klinikums oder auch an Dritte nur im Zusammenhang mit der Erfüllung des Verarbeitungszweckes weitergegeben werden. Für die Übermittlung an externe Stellen/ Personen muss eine Zulässigkeit in Form einer Auftragsverarbeitungsvereinbarung oder einer anderen konkret zu benennenden Rechtsgrundlage bestehen.
Betroffene Personen müssen über die Rechtsgrundlage der Verarbeitung ihrer Daten sowie über interne und externe Empfänger unterrichtet werden.

5.2.2. Zweckbindung

Personenbezogene Daten sind für klar und ausdrücklich angegebene und rechtmäßige Zwecke zu erfassen und zu verarbeiten und dürfen auch später nicht ohne eine entsprechende Rechtsgrundlage abweichend von diesen Zwecken verwendet oder weiterverarbeitet werden.
Betroffene Personen müssen über den Zweck der Verarbeitung unterrichtet werden.

5.2.3. Datenminimierung

Die für die Verarbeitung erhobenen personenbezogenen Daten müssen für den benannten Zweck erforderlich sein und auf das für die Erreichung des Verarbeitungszweckes notwendige Maß beschränkt sein.
Betroffene Personen müssen über die gespeicherten Daten bzw. Datenkategorien unterrichtet werden.

5.2.4. Richtigkeit

Die für den Verarbeitungszweck erhobenen und gespeicherten Daten müssen sachlich richtig und auf einem aktuellen Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf den Verarbeitungszweck falsch sind, unverzüglich gelöscht oder berichtigt werden.

5.2.5. Speicherbegrenzung

Personenbezogene Daten dürfen nur solange gespeichert werden, wie sie zur Erfüllung des Verarbeitungszweckes erforderlich sind oder gemäß gesetzlichen Anforderungen aufzubewahren sind. Werden die personenbezogenen Daten für den Verarbeitungszweck nicht länger benötigt und existiert keine gesetzlich geregelte Aufbewahrungsfrist sind die Daten zu löschen oder zu anonymisieren.
Die Fachbereiche haben für gespeicherte personenbezogene Daten zum Zeitpunkt der Erhebung die Speicherdauer festzulegen und nach deren Ablauf eine automatische oder manuelle Löschung durchzuführen.
Betroffene Personen müssen über die Speicherdauer unterrichtet werden. Ist dies nicht möglich, sind ihnen die Kriterien zur Festlegung der Speicherdauer mitzuteilen.

5.2.6. Wahrung von Integrität und Vertraulichkeit

Bei der Datenverarbeitung muss eine angemessene Sicherheit der personenbezogenen Daten gewährleistet werden. Dies verlangt insbesondere einen angemessenen Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch die Umsetzung von dazu geeigneten technischen und organisatorischen Schutzmaßnahmen. Das Klinikum hat angemessene technische und organisatorische Schutzmaßnahmen realisiert und diese in Form eines zentralen Sicherheitskonzeptes dokumentiert.
Soweit Fachbereiche von diesen Standardmaßnahmen abweichen sind sie verpflichtet schriftlich nachzuweisen, dass für die betreffende Verarbeitung ein zu den zentralen Schutzmaßnahmen vergleichbares Schutzniveau gewährleistet wird.

5.3. Informationspflicht gegenüber dem Betroffenen

Gemäß dem Art. 12 DSGVO müssen die von einer Datenverarbeitung betroffenen Personen über die Verarbeitung ihrer Daten in kurzer und präziser, leicht zugänglicher und leicht verständlicher Form über Art und Umfang der Datenverarbeitung informiert werden. Die konkreten Inhalte der bereitzustellenden Information ergeben sich aus den Art. 13 (Direkterhebung) und Art. 14 DSGVO (Erhebung bei Dritten). Bei der Informationspflicht im Falle der Direkterhebung wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DSGVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DSGVO).
Die Bereitstellung der Informationen erfolgt in der Regel schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person nachgewiesen wurde.
Das Klinikum verwendet zur Erfüllung der Informationspflichten gegenüber den Betroffenen Informationsblätter, die als zentrale Vorlagen über das Krankenhausinformationssystem (Patienten und Besucher) sowie im Sharepoint (Beschäftigte) bereitgestellt werden und durch die jeweilige Fachabteilung ggf. hinsichtlich der jeweiligen Verarbeitung anzupassen sind. Die durch die Fachbereiche erstellten Informationsblätter sind mit dem DSB vorab abzustimmen.

5.4. Verarbeitung besonderer personenbezogener Daten

Personenbezogene Daten, die ihrer Art nach in besonderem Maße die Selbstbestimmung und persönlichen Freiheitsrechte einer Person berühren und daher besonders sensibel sind, erfordern einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten des Betroffenen auftreten können.
Personenbezogene Daten sind dann als besonders sensibel einzustufen, wenn sie Aufschluss über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit sowie Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung des Betroffenen geben. Dies gilt ebenso für die genetischen oder biometrischen Daten, die zur eindeutigen Identifizierung einer natürlichen Person geeignet sind.
Die Verarbeitung solcher personenbezogenen Daten ist grundsätzlich nach Art. 9 DSGVO verboten und nur in ganz bestimmten Ausnahmefällen zulässig. Ihre Verarbeitung unterliegt einer besonderen Pflicht zur Sorgfalt und Überprüfung.
Das Klinikum darf besonders sensible Daten unter folgenden Voraussetzungen verarbeiten:

- nur mit ausdrücklicher Genehmigung der betroffenen Person nach entsprechendem Hinweis auf die Sensibilität der Daten oder
- basierend auf nationalen bzw. europäischen Gesetzen, die eine Verarbeitung ausdrücklich erlauben, wie z. B. einem Vertrag oder gesetzlicher Melde- und Übermittlungspflichten / -befugnisse.

Für die Datenverarbeitung des Klinikums relevante besonders sensible Daten sind vorrangig:

- Angaben zur rassischen/ ethnischen Herkunft
- Gesundheitsdaten sowie
- ggf. zukünftig genetische oder biometrische Daten zum Zweck der eindeutigen Identifizierung

Die folgenden Arten der Risikoverarbeitung bedürfen darüber hinaus einer besonderen Überprüfung:

- bei der Verknüpfung von Daten für unterschiedliche Zwecke;
- bei Einsatz von risikobehafteter Technologie (z. B. Cloudbasierte Datenverarbeitung)
- bei der Übertragung personenbezogener Daten nach außerhalb der Europäischen Union

Die Anlage 1 „Besondere Kategorien personenbezogener Daten“ enthält hierzu weitere Hinweise und Vorgaben.

5.5. Schadensstufen im Datenschutz

Im Umgang mit personenbezogenen Daten (Art. 6 DSGVO) und hier im speziellen mit besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) ist grundsätzlich ein hohes Schutzniveau zu gewährleisten.
Die Art. 33, 34 DSGVO beschreiben die Maßnahmen, die im Falle einer unbefugten Offenbarung zu ergreifen sind. Ein intern etablierter Meldeprozess stellt das sicher. Im Rahmen der Aufarbeitung von Datenpannen und bei der Ableitung von Schutzmaßnahmen im Kontext einer Datenschutzfolgeabschätzung sind die Folgen für den Betroffenen im Falle einer unbefugten Kenntnisnahme der Daten durch Dritte oder Schädigung bzw. Verlust der Daten abzuschätzen und zu bewerten.
Hierfür wurden interne Schadensstufen definiert, die das Ausmaß des zu erwartenden Schadens bei dem Betroffenen – im Falle einer unbefugten Offenbarung – beschreiben.

Das Klinikum unterscheidet aus Datenschutzsicht zwischen 5 Schadensstufen:

Schadensstufe	**Personenbezogene Daten,**
A	die von den Betroffenen frei zugänglich gemacht wurden.
B	deren unsachgemäße Handhabung zwar **keine besondere Beeinträchtigung** erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **beeinträchtigen** könnte („Ansehen”).
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **erheblich beeinträchtigen** könnte („Existenz”).
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.

Die Mehrzahl der im Klinikum verarbeiteten Informationen / Daten wird der Schadensstufe C oder D zugeordnet.

In der DA Klassifizierung von Informationen wird dies mit Bezug zu den Vertraulichkeitsklassen zusammenfassend dargestellt.

5.6. Sicherheit der Datenverarbeitung

Zur Einhaltung der Sicherheitsziele und damit zum Schutz der personenbezogenen Daten vor unbefugter oder unrechtmäßiger Kenntnisnahme/ Verarbeitung/ Zugriff/ Verfälschung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung sind geeignete Schutzmaßnahmen in Abhängigkeit der betrachteten Verarbeitungstätigkeit und der mit damit verbundenen möglichen Risiken zu ergreifen.

5.6.1. Umgang mit personenbezogenen Daten

Die Informationen und Daten des Klinikums benötigen nicht alle den gleichen Schutz. Für einen wirtschaftlich sinnvollen und dem Risiko angemessenen Schutz werden Informationen/ Daten unterschiedlich klassifiziert. Anhand der DA Klassifizierung von Informationen wird die Vertraulichkeitsklasse sowie der konkrete Umgang mit diesen Daten bzw. die erforderlichen Schutzmaßnahmen klinikumsweit festgelegt. Anhand der genannten Beispiele können weitere Informationen einer der Vertraulichkeitsklassen zu geordnet werden. Im Zweifel ist die Stabsstelle Informationssicherheit hinzuziehen.

5.6.2. Risikoanalyse

Für jedes Verarbeitungsverfahren /jede Verarbeitungstätigkeit ist anhand der verarbeiteten Daten die Zuordnung zu einer Schutzstufe vorzunehmen sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken (Risiko-/ Gefährdungsanalyse) zu erstellen. Diese orientiert sich an der Art, dem Umfang, den Umständen und Zwecken der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schadenswirkung einer bestehenden Gefahr. Die Analyse ist aus dem Blickwinkel des Betroffenen hinsichtlich der möglichen Gefährdungen vorzunehmen.
In der Verfahrensanweisung „Risikoanalyse Informationssicherheit“ werden die Vorgehensweise für die Durchführung einer Risikoanalyse beschrieben und die zur Durchführung erforderlichen Arbeitsblätter zur Verfügung gestellt.

5.6.3. Sicherheitskonzept

Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist durch die IT-Abteilung in Abstimmung mit dem DSB ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risiko-/ Gefährdungsanalyse. Das Sicherheitskonzept ist maßgeblich für die weitere Behandlung der festgestellten Risiken.
Die tatsächlichen Maßnahmen hängen von den verarbeiteten personenbezogenen Daten, von den vorhandenen Risiken, den möglichen Folgen für die betroffene Person, den verfügbaren technischen und organisatorischen Schutzmaßnahmen ab.
Neben dem Sicherheitskonzept sind ergänzende Regelungen in der Anlage 2 aufgeführt. Diese Aufstellung wird ständig ergänzt.

5.6.4. Verarbeitungsgestaltung

Die technisch-organisatorischen Maßnahmen haben sich an den Grundsätzen des Datenschutzes durch Technik (Data Protection by Design) und an datenschutzfreundlichen Voreinstellungen (Data Protection by Default) auszurichten.

Hier geht es insbesondere um die Einhaltung von Grundsätzen, wie z. B. Datenminimierung, durch die Verwendung von technischen Gestaltungsmöglichkeiten sowie durch die aktive Nutzung von vorhandenen Möglichkeiten zur Voreinstellung von Systemen, wie z. B. eine starke Benutzerauthentifizierung.

- **Data Protection by design/ Datenschutz durch Technikgestaltung:**

  Es sind zum frühestmöglichen Zeitpunkt der Gestaltung von Verarbeitungsvorgängen technische und organisatorische Maßnahmen zu treffen, die darauf ausgelegt sind, die Privatsphäre zu schützen und Datenschutzgrundsätze von Beginn an zu garantieren.
  Dies erfordert die Einbindung des Datenschutzes in technologische Systeme und Lösungen zum frühestmöglichen Zeitpunkt der Entwicklung.

- **Data Protection by default/ Datenschutzfreundliche Voreinstellung:**

  Es ist durch Voreinstellungen am genutzten IT-System/ an der genutzten Anwendung sicherzustellen, dass personenbezogene Daten mit dem größtmöglichen Datenschutz (zum Beispiel sollten ausschließlich benötigte Daten verarbeitet werden, kurze Speicherfristen, begrenzte Zugänglichkeit und eine starke Authentifizierung vorgesehen werden) verarbeitet werden, damit diese Daten von vornherein nicht einer unbestimmten Zahl von Personen zugänglich gemacht werden.
  Dies betrifft hauptsächlich das Prinzip der Datenbeschränkung und -minimierung (die erhobenen Daten werden für den Zweck der Datenverarbeitung unbedingt benötigt), die Datenspeicherung (im Zusammenhang mit dem Zweck der Datenverarbeitung) und die Pseudonymisierung/ Anonymisierung von Daten.

Im Rahmen der Änderung bzw. Neugestaltung von Verarbeitungstätigkeiten sind die oben genannten Datenschutzgrundsätze zu berücksichtigen.

5.6.5. Datenschutzfolgeabschätzung

Eine Datenschutzfolgeabschätzung (DSFA) ist eine erweitere Risikoanalyse, die immer dann durchzuführen ist, wenn im Rahmen der regulären Risikoanalyse für die Rechte und Freiheiten der Betroffenen durch eine Verarbeitungstätigkeit ein hohes verbleibendes Restrisiko festgestellt wird (Art. 35 Abs. 1 DSGVO). Darüber hinaus wurde durch die zuständige Datenschutzaufsichtsbehörde eine Übersicht von Verarbeitungstätigkeiten (Black List) öffentlich zur Verfügung gestellt, für die zwingend eine DSFA vor der Nutzung durchzuführen ist.
Die Durchführung der DSFA dient dazu, in einem systematischen Vorgehen geplante Verarbeitungsvorgänge zu beschreiben, ihre Notwendigkeit und Verhältnismäßigkeit zu beurteilen, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und zur Bewältigung dieser Risiken vorab Abhilfemaßnahmen festzulegen. Grundsätzlich darf ein Verarbeitungsvorgang solange nicht durchgeführt werden, wie ein hohe Restrisiko besteht.
Die Folgenabschätzung ist von dem für die Verarbeitung zuständigen Fachbereich unter Einbindung des Datenschutzteams und des DSB sowie ggf. eines in die Verarbeitung eingebundenen Dienstleisters durchzuführen. Die Mindestinhalte der DSFA ergeben sich aus Art. 37 Abs. 7 DSGVO. Die Verfahrensanweisung „Risikoanalyse Informationssicherheit regelt die konkrete Durchführung und die erforderlichen Arbeitsschritte.
Wird nach Durchführung des DSFA weiterhin ein hohes verbleibendes Restrisiko für die von der Verarbeitung betroffenen Personen festgestellt, so ist die zuständige Datenschutzaufsichtsbehörde zwecks Beratung und Abstimmung zu kontaktieren.
Die Verarbeitungstätigkeit darf erst nach Abschluss der Abstimmung mit der Behörde und Beseitigung des hohen Restrisikos begonnen werden.

5.7. Transparenz und Dokumentation der Datenverarbeitung

Über Verfahren und Verarbeitungstätigkeiten, die den Umgang mit personenbezogenen Daten betreffen, führt das Klinikum ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO. Der für ein Verfahren Verantwortliche bzw. der zuständige Datenschutzkoordinator meldet Verarbeitungstätigkeiten zeitnah gemäß den vom DSB definierten Vorgaben und bereitgestellten Erhebungsbögen. Gleiches gilt für wesentliche Veränderungen an der Verarbeitungstätigkeit (Change Request).
Unabhängig von dieser Meldung ist der DSB bereits frühzeitig bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Verarbeitungstätigkeit (Anwendung)sowie die Erfüllung der Benachrichtigungspflicht gegenüber den Betroffenen zu informieren. Bei standardisierten Erhebungen (Erhebungsbögen, Fragebögen, Online-Eingabefelder auf Websites etc.) ist der Erhebungsbogen etc. dem DSB zur Abstimmung vorzulegen.
Soweit der DSB feststellt, dass die beabsichtigte Verarbeitung einer Datenschutzfolgeabschätzung unterliegt, teilt er dies umgehend mit.

5.8. Schutzrechte der Betroffenen

Die Informationspflichten gemäß DSGVO bilden die Basis für die Ausübung der Betroffenenrechte. Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben.
Neben allgemeinen Fragen zum Datenschutz in unserem Unternehmen und dem Wunsch den Datenschutzbeauftragten sprechen zu wollen, kann es im Zusammenhang mit der Inanspruchnahme der sogenannten Betroffenenrechte (Art. 7 Abs. 3, Art. 15 – 21 DSGVO) auch ganz konkret zu folgenden Anfragen kommen:

- Auskunft (Art. 15) über die zur eigenen Person gespeicherten Daten (die häufigste Anfrage),
- Berichtigung (Art. 16) von Daten,
- Löschung (Art. 17) von Daten,
- Einschränkung (Art. 18) der Verarbeitung (Sperrung),
- Mitteilungspflicht (Art. 19) über Empfänger bei Berichtigung, Löschung und Einschränkung
- Bereitstellung der Daten in elektronischer Form (Datenübertragbarkeit, Art.20),
- Widerspruch gegen die Verarbeitung von Daten (Art. 21), sowie auch
- Widerruf von erteilten Einwilligungen (Art. 7 Abs. 3).

Macht ein Betroffener von seinen Schutzrechten (z. B. Auskunftsrecht oder Löschung) nach der DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung unter Abstimmung mit dem betroffenen Fachbereich und dem DSB durch das Datenschutzteam. Die Betroffenenrechte von Beschäftigten werden durch die Personalverwaltung erfüllt. Der Ablauf der Bearbeitung von Betroffenenanfragen ist in der Verfahrensbeschreibung „Bearbeitung von Betroffenenanfragen“ verbindlich geregelt. Es ist sicherzustellen, dass die Betroffenenrechte in der Regel innerhalb von 4 Wochen nach Eingang der Anforderung erfüllt werden. Ist dies im Ausnahmefall nicht möglich, so sind dem Betroffenen noch innerhalb der 4-Wochenfrist die Gründe für die Verzögerung schriftlich mitzuteilen. Die Anfrage muss dann aber zwingend innerhalb der nächsten 8 Wochen zum Abschluss gebracht werden.

5.9. Umgang mit Datenschutzpannen

Im Falle einer Datenschutzverletzung besteht seitens des Klinikums nach Art. 33 DSGVO eine grundsätzliche Meldepflicht gegenüber der Datenschutzaufsichtsbehörde. Eine Datenschutzpanne ist innerhalb von 72 Stunden nach Bekanntwerden des Vorfalles über die behördliche Website an

die zuständige Datenschutzaufsichtsbehörde zu melden. Um diese gesetzliche Verpflichtung erfüllen zu können gilt eine unternehmensinterne Meldepflicht von datenschutzrelevanten Vorkommnissen.
Eine Datenschutzpanne (offizielle Bezeichnung: Verletzung des Schutzes von personenbezogenen Daten) ist eine „Verletzung der Sicherheit, die ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt, unabhängig davon ob die Daten übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden." (Art. 4 Nr. 12 DSGVO). Zur weiteren Definition des Begriffes „Verarbeitung" siehe Art. 4 Nr. 2 DSGVO).
Es ist unerheblich ob es sich um „einfache" personenbezogene Daten oder um besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO handelt. Entscheidend ist, dass die Daten Dritten unzulässiger Weise zur Kenntnis gelangen, unabhängig davon, ob dies vorsätzlich oder fahrlässig erfolgte.
Eine „Verletzung der Sicherheit" betrifft auch die rechtwidrige Datenverarbeitung, wenn dadurch eine Offenlegung an Dritte erfolgt. Eine Datenschutzverletzung liegt ebenfalls vor, wenn personenbezogene Daten infolge eines Sicherheitsbruches längere Zeit unerreichbar waren oder dauerhaft gelöscht wurden.
Üblicherweise werden potentielle Datenschutzvorfälle durch interne Stellen (Beschäftige des Klinikums) oder durch externe Stellen (Patienten, Dienstleister, Behörden, sonstige Stellen oder Personen) festgestellt und gegenüber dem Klinikum geäußert. Die Überprüfung und Bearbeitung solcher Hinweise erfolgt an zentraler Stelle im Unternehmen.
Für alle Beschäftigten besteht eine Mitwirkungspflicht hinsichtlich der Aufklärung von Datenschutzpannen. Meldeberechtigt sind alle Beschäftigen des Klinikums.

Hinweise, die durch Patienten, Dienstleister und sonstige externe Stellen / Personen eingehen sind ebenfalls an die genannte Email-Adresse weiterzuleiten.
Um eine fristgerechte Bearbeitung zu gewährleisten, haben auf dieses Email-Konto folgende Stellen Zugriff:

- die/der Datenschutzbeauftragte
- das Datenschutzteam

Die weitere Bearbeitung von gemeldeten Datenschutzvorfällen regelt die Verfahrensanweisung Umgang mit Datenschutzmeldungen.

5.10. Verpflichtung, Schulung und Sensibilisierung

Alle Beschäftigten, die Umgang mit personenbezogenen Daten haben, werden auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie verpflichtet. Neue Mitarbeiter werden zum Arbeitsantritt entsprechend durch die Personalabteilung verpflichtet. Die Notwendigkeit zur Verpflichtung besteht auch gegenüber Aushilfen, Leiharbeitnehmer, Fremdkräfte, Praktikanten etc.
Die Verpflichtung erfolgt unter Verwendung des zentralen Formulars „Verpflichtungserklärung_Datenschutz" (im Sharepoint) unter Aushändigung des von dem DSB erstellten Merkblatts durch die Personalabteilung.
Mitarbeiter, die besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz - TKG) unterliegen, werden von den Vorgesetzen ergänzend schriftlich verpflichtet. Die jeweilige Verpflichtungserklärung ist zur Personalakte zu nehmen.
Der DSB ist über die Verpflichtung von Mitarbeitern, die erfolgte Belehrung und den konkreten Arbeitsplatz zwecks Feststellung eines evtl. Nachschulungs- oder Kontrollbedarfes zu informieren.

Den Mitarbeitern ist durch die zuständige Fachabteilung die Möglichkeit zur Teilnahme an den zentral angebotenen Datenschutzschulungen einzuräumen. Für ggf. in Abstimmung zwischen der Fach-

abteilung und dem DSB geplante Präsenzschulungstermine sind die betroffenen Mitarbeiter freizustellen. Die Schulung ist regelmäßig zu wiederholen, üblicherweise jährlich. Über die Teilnahme ist ein Nachweis zu führen. Die Schulung kann auch in Form einer Online-Schulung erfolgen.

5.11. Auftragsverarbeitung

Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung, Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten erhalten können, so ist der DSB vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DSGVO genügenden Vertragsentwurfs und der Kriterien (Nachweis der technisch – organisatorischen Maßnahmen, Verzeichnis der Verarbeitungstätigkeit als Auftragsverarbeiter) der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren. Das erforderliche Vertragsmuster „Auftragsverarbeitung nach Art. 28 DSGVO“ steht als Standardvorlage zur Verfügung.

Sobald im Rahmen einer Dienstleistung personenbezogene Daten verarbeitet werden ist der Abschluss eines AV-Vertrages unbedingte Vertragsgrundlage.

Entsprechendes gilt, falls das Klinikum selbst als Dienstleister Tätigkeiten im Auftrag eines Dritten ausführt.

5.12. Sanktion bei Verstößen und Zuwiderhandlungen

Jeder Verstoß oder eine Zuwiderhandlung gegen die Datenschutzgrundsätze kann mit Sanktionen und Bußgelder durch die Datenschutzaufsichtsbehörde geahndet werden. Die Bußgelder können je nach Verstoß bis zu 20 Mio. Euro betragen bzw. 2 bis 4 Prozent des Vorjahresumsatzes. Als weitere Maßnahmen können Verarbeitungstätigkeiten durch die Aufsichtsbehörden untersagt oder mit Auflagen/ Beschränkungen belegt werden.

5.13. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben der DSGVO und des BDSG, die durch diese Richtlinie auf die betrieblichen Abläufe des Klinikums übertragen werden, muss gemäß der Rechenschaftspflicht nach Art. 5 DSGVO jederzeit nachweisbar sein.
Der Grundsatz der Rechenschaftspflicht ist durch jede Klinik und jede Fachabteilung für die durchgeführte Verarbeitung personenbezogener Daten einzuhalten. Die Fachbereiche müssen jederzeit nachweisen können, dass sie die Grundsätze der Verarbeitung personenbezogene Daten (siehe Kapitel 5.2) einhalten. Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich des Verarbeitungszweckes, der verarbeiteten Daten, der rechtlichen Zulässigkeit, der Speicherbefristung, der Festlegung des Empfängerkreises, der getroffenen Maßnahmen und der dazugehörigen Abwägungen bezüglich deren Angemessenheit und Wirksamkeit zu erfolgen.
Im Wesentlichen müssen die Klinik und Fachabteilungen geeignete und effektive Maßnahmen umsetzen, um die Konformität der Datenverarbeitung sowie die Wirksamkeit der ergriffenen Maßnahmen nachweisen zu können.
Aus der Rechenschaftspflicht ergibt sich insbesondere die Notwendigkeit für die Einführung und kontinuierliche Pflege des Verzeichnisses der Verarbeitungstätigkeiten, den Einsatz von datenschutzfreundlichen Systemvoreinstellungen und datenschutzfreundlicher Technikgestaltung (Data Protection by default, Data Protection by design) sowie von risikoorientierten Schutzmaßnahmen und Datenschutzfolgenabschätzungen.

6. Datenschutzmanagementsystem

Zur Unterstützung aller Bereiche und um eine effiziente und kontinuierlich verbesserte Anwendung des Datenschutzes im Unternehmen zu gewährleisten, ist ein Datenschutzmanagementsystem (DSMS) im Unternehmen etabliert. Das Managementsystem, das selbst einem qualitativen Überwachungsprozess unterliegt, gilt für alle Unternehmensbereiche. Die formale Verantwortlichkeit für das DSMS liegt beim Direktorium. Das Datenschutzteam und der Datenschutzbeauftragte gestalten das Managementsystem aus.
Das DSMS sieht verschiedene Aktivitäten vor, mit denen die Beachtung der Grundsätze und der rechtlichen Vorgaben durch alle Beschäftigten gemessen werden soll.
Dazu gehören:

- Einhaltung der Datenschutzgrundsätze und Lenkungsvorgaben
- Durchführung von Schulungen und Sensibilisierungsmaßnahmen
- Beachtung gesetzlicher Bestimmungen zur Datenverarbeitung
- Durchführung der Informationspflichten und der Betroffenenrechte
- Durchführung von Risikoanalysen und Datenschutzfolgeabschätzung
- Durchführung einer sicheren Datenverarbeitung
- Umgang mit Datenpannen

Zur angemessenen Umsetzung und Erreichung dieser Grundsätze werden durch das Klinikum die folgenden Mittel eingesetzt.

6.1. Schulung und Sensibilisierung der Beschäftigten

Das grundlegende Wissen über den Datenschutz, die Anforderungen an die Verarbeitung von personenbezogenen Daten und die Schutzrechte von Betroffenen werden allen Beschäftigten durch zentrale und dezentrale Schulungs- und Sensibilisierungsmaßnahmen vermittelt und regelmäßig wiederholt. Insbesondere die Auffrischung des Wissens erfolgt sowohl durch zentrale als auch dezentrale Aktionen. Verantwortlich hierfür sind das Datenschutzteam, der Datenschutzbeauftragte und die Datenschutzkoordinatoren. Die organisatorische Verantwortung für die Schulungsplanung liegt bei den Leitungspersonen. Zu ausgewählten Themenstellungen werden bereichsübergreifende zentral organisierte Aktionen durchgeführt. Die Aktionen können auf dezentraler Ebene durch Aktionen der Fachbereiche ergänzt werden.
Die DSKen haben eine Grundlagenschulung erhalten. Um die zur Erfüllung ihrer Aufgaben erforderlichen Sachkenntnisse zu erlangen, erhalten die DSKen darüber hinaus Informationen und Materialien im Rahmen der Sitzungen des Arbeitskreises.

6.2. Überprüfung und Auditierung

Durch das Klinikum ist die Beachtung der Datenschutzgrundsätze sowie der Datenschutzgesetze regelmäßig intern zu überprüfen. Das Direktorium delegiert diese Aufgabe an die Chefärzte und Abteilungsleiter, die zu ihrer Unterstützung den benannten DSK mit einbinden können. Auch das Datenschutzteam und der Datenschutzbeauftragte sind berechtigt derartige Überprüfungen durchführen.
Zur Überprüfung gehört die Einschätzung und Kontrolle der Möglichkeiten des Prozess- und Datenzugriffs sowie z. B. der Einhaltung der Zweckbindung, der Wahrung der Vertraulichkeit, der technisch-organisatorischen Sicherheitsmaßnahmen, der Zulässigkeit der Verarbeitung, der Aufbewahrungsfristen, der Sicherstellung der Informations- und Betroffenenrechte, der Durchführung der Risikoanalyse und Folgenabschätzung.
Neben internen Audits kann das Klinikum zur Unterstützung der Entwicklung des DSMS auch externe Audits durch geeignete Dienstleistungsunternehmen beauftragen.

6.3. Transparenz und Dokumentation der Datenverarbeitung

Hinsichtlich des Prinzips der Transparenz und Dokumentation der Datenverarbeitung und um die von der Datenverarbeitung betroffenen Personen hinsichtlich der Wahrnehmung ihrer Schutzrechte, insbesondere das Recht auf Auskunft, zu unterstützen, führt das Klinikum eine Übersicht aller Verarbeitungstätigkeiten und hält diese durch jährliche Überprüfungen aktuell.
Neben der Bereitstellung einer umfassenden Übersicht wird so auch die Basis für eine Kontrolle der Datenverarbeitung geschaffen. Für das Unternehmen wird mit dem Verzeichnis auch der Umgang mit Auskunftsanfragen von betroffenen Personen sowie deren Bearbeitung erleichtert.

6.4. Bearbeitung von Datenschutzanfragen

Anfragen zum Datenschutz im Klinikum, unabhängig davon ob diese durch interne oder externe Personen gestellt werden, müssen unverzüglich einer Bearbeitung zugeführt werden. Anfragen zu den Betroffenenrechten, z. B. Auskunft, Löschung etc., sind grundsätzlich innerhalb der gesetzlich definierten Frist von 4 Wochen zu bearbeiten. Alle Anfragen werden durch das Datenschutzteam unter Einbindung der betroffenen Klinik / Fachabteilung und des Datenschutzbeauftragten bearbeitet und dokumentiert.

6.5. Bearbeitung von Datenschutzvorfällen

Alle Beschäftigten sind verpflichtet Datenschutzvorkommnisse an das Datenschutzteam sowie den Datenschutzbeauftragten per Meldeformular / Email zu melden. Externe Meldungen können über die veröffentlichte Email-Adresse datenschutz@klinikum.wolfsburg.de eingehen und werden in gleicher Weise wie interne Hinweise bearbeitet.
Sobald die mögliche Auswirkung des Vorfalls auf den Datenschutz ersichtlich ist, muss durch das Klinikum in Abstimmung mit dem DSB entschieden werden, ob es sich um eine meldepflichtige Datenschutzpanne handelt und der Vorfall unter Verwendung der behördlichen Meldeformulare oder dem offiziellen Meldeportal so bald als möglich, mindestens aber innerhalb des Zeitfensters von 72 Stunden, an die zuständige Datenschutzaufsichtsbehörde gemeldet werden.
Intern wird jeder Vorfall in einer Übersicht der Datenschutzvorfälle dokumentiert und aufgearbeitet. Hierbei stehen Ursachenklärung und Maßnahmenbehandlung, z. B. durch technisch-organisatorische Anpassungen, Schulung und Sensibilisierung etc., zur zukünftigen Vermeidung vergleichbarer Ereignisse im Fokus.

6.6. Auftragsverarbeitung durch Dienstleister

Soweit Dienstleister im Rahmen ihrer Leistungserbringung für das Klinikum personenbezogene Daten im Auftrag verarbeiten oder nur zur Kenntnis nehmen können, sind neben dem eigentlichen Leistungsvertrag die datenschutzrelevanten Aspekte nach Art. 28 DSGVO sowie die Verschwiegenheitspflicht nach § 203 StGB ebenfalls in Form einer schriftlichen Vereinbarung zu regeln. Darüber hinaus muss das Klinikum einen Auswahl- und Prüfprozess etablieren, um die Eignung von Dienstleistern unter Datenschutzaspekten bewerten zu können. In diesen Prüfprozess sind die technischen und organisatorischen Schutzmaßnahmen, die durch den Dienstleister realisiert werden, einzubeziehen. Das Ergebnis der Auswahl und Überprüfung ist nachvollziehbar zu dokumentieren und unterliegt dem kontinuierlichen Verbesserungsprozess.

6.7. Risikobetrachtung und Folgenabschätzung

An die Dokumentation der Verarbeitungstätigkeiten schließt sich immer auch eine risikoorientierte Bewertung der betrachteten Prozesse an, um die relevanten Gefährdungen für die Persönlichkeits- und Freiheitsrechte der Betroffenen zu ermitteln. Hierbei sind anerkannte objektivierte Methodiken

zu verwenden. Im Anschluss sind geeignete Maßnahmen zur Risikobehandlung, in der Regel in der Form einer Minimierung oder Vermeidung, zu ergreifen. Die Risikoermittlung sowie deren Behandlung sind nachvollziehbar zu dokumentieren.
Bei einem verbleibenden hohen Risiko für die Betroffenen oder für Verarbeitungen, die in der behördlich veröffentlichten Blacklist eingetragen sind, ist zwingend eine Datenschutzfolgenabschätzung durchzuführen. Die Folgenabschätzung sowie deren Ergebnis sind schriftlich zu dokumentieren. Kann das Risiko nicht reduziert werden sind Konsultationen mit der Datenschutzaufsichtsbehörde aufzunehmen.

6.8. Wirksamkeit des DSMS und kontinuierliche Verbesserung

Alle Maßnahmen im Zusammenhang mit dem Datenschutzmanagementsystem unterliegen einer kontinuierlichen qualitativen Überwachung die in der Verfahrensanweisung „Kontinuierlicher Verbesserungsprozess“ detailliert beschrieben ist. Die aus den Prüfungen gewonnenen Erkenntnisse werden genutzt, um die bestehenden Regelungen und Prozesse in Inhalt und Darstellung zu ergänzen bzw. zu verbessern. Die angepassten Regelungen und Prozesse unterliegen ebenfalls dem kontinuierlichen Verbesserungsprozess mit den Einzelschritten „Plan“, „Do“, „Check“ und „Act“ und werden somit wiederum im nächsten Prüfungszyklus hinsichtlich Angemessenheit und Wirkung kontrolliert.

7. Inkrafttreten

Diese Richtlinie tritt zum 01.07.21 in Kraft.

W. Köster Klinikumsdirektor	Prof. Dr. M. Menzel Ärztlicher Direktor	C. Bitter Pflegedirektorin

8. Dokumentenhistorie

Datum	Version	Autor	Bemerkung/ Änderung
10.06.2021	001	H.Opel / R.Gruetz	Dokument finalisert
16.06.2021	001	Direktorium	Freigabe

9. Anlage 1 Besondere Kategorien personenbezogener Daten

Stand 15.01.2021

Definition

Art. 9 der EU-Datenschutzgrundverordnung (DSGVO) definiert Datenkategorien, deren Daten einem besonderen Schutz unterliegen.

Bei diesen Datenkategorien handelt es sich um personenbezogener Daten, aus denen die rassische und 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.

Besonders schutzbedürftig sind somit alle Angaben, die direkt oder indirekt Informationen zu den in Art. 9 DSGVO angegebenen Datenkategorien vermitteln (z. B. Einnahme von Medikamenten, körperliche oder geistige Verfassung, regelmäßiger Besuch einer bestimmten Kirche). Andererseits wird nicht jede mittelbare Angabe zu den besonderen Kategorien personenbezogener Daten die Anwendung der speziellen (strengen) Verarbeitungsbestimmungen nach sich ziehen – z. B. ist bloßer Alkoholkonsum im Gegensatz zu einer Alkoholabhängigkeit kein Gesundheitsdatum, der rein geographische Geburtsort keine Angabe über die rassische oder ethnische Herkunft und der einmalige Besuch eines Sakralbaus enthält keine Aussage über eine religiöse Überzeugung.

Verarbeitungsverbot mit Ausnahmevorbehalt

Art. 9 Abs. 1 DSGVO bestimmt ein grundsätzliches Verbot der Verarbeitung von Daten dieser Kategorien.

In Art. 9 Abs. 2 lit. a bis j DSGVO werden allerdings umfangreiche Ausnahmen von diesem Grundsatz geregelt.

Neben der ausdrücklichen Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) kommen besondere Rechtsvorschriften oder spezielle Umstände im Einzelfall als Rechtfertigung für die Verarbeitung besonders schutzbedürftiger Angaben in Betracht.

Das Verarbeitungsverbot gilt gemäß Art. 9 Abs. 2 daher weiterhin nicht, wenn die Verarbeitung gemäß lit. b bis lit. j:

b) für die Ausübung von Rechten und Pflichten aus dem Arbeits- oder Sozialrecht erforderlich ist. Solche Verarbeitungen dürfen jedoch nur dann stattfinden, wenn sie nach einer Rechtsvorschrift erforderlich sind. Davon umfasst sind auch Kollektivvereinbarungen wie Betriebsvereinbarungen. Die Rechtsvorschriften müssen geeignete Garantien für die Grundrechte und die Interessen der betroffenen Personen vorsehen (s. a. ErwGr. 52);

c) zum Schutz lebenswichtiger Interessen einer Person erforderlich ist und diese körperlich oder rechtlich außerstande ist einzuwilligen;

d) auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung/Vereinigung/ Organisation ohne Gewinnerzielungsabsicht erfolgt und sich ausschließlich auf aktuelle oder ehemalige Mitglieder oder auf Personen bezieht, die mit der Stelle regelmäßig Kontakte im Zusammenhang mit deren Tätigkeitszweck unterhalten, und die Daten nicht ohne Einwilligung nach außen weitergegeben werden;

e) Daten betrifft, die die betroffene Person offensichtlich öffentlich gemacht hat;

f) zur Rechtsverfolgung oder für die Aufgabenerfüllung der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;

g) auf rechtlicher Grundlage aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist;

h) für Zwecke der Gesundheitsvorsorge, der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich erforderlich ist, durch Berufsgeheimnisträger erfolgt und auf einer rechtlichen Grundlage oder aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes beruht;

i) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, z. B. zur Verhinderung von Epidemien oder zur Gewährleistung der Arzneimittelsicherheit, auf rechtlicher Grundlage erforderlich ist;

j) auf rechtlicher Grundlage für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO erforderlich ist. Von den in Art. 9 Abs. 2 lit. b, g, h, i und j DSGVO benannten Öffnungsklauseln hat der Bundesgesetzgeber in den §§ 22 Abs. 1, 27 und 28 BDSG in Verbindung mit den jeweiligen konkreten spezialgesetzlichen Regelungen Gebrauch gemacht. § 22 Abs. 2 BDSG enthält darüber hinaus beispielhaft aufgezählte Maßnahmen zur Wahrung der Interessen der betroffenen Personen, die jeden Verantwortlichen und damit jeden, der besondere Kategorien personenbezogener Daten verarbeitet, treffen.

Weitere Anforderungen an die Datenverarbeitung

Zusätzlich zu den speziellen Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten sollen nach ErwGr. 51 die allgemeinen Grundsätze und andere Bestimmungen der DSGVO, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung gelten. Bei besonders schutzbedürftigen Daten ist die Eingriffsintensität regelmäßig höher, weshalb höhere Anforderungen an die Rechtfertigung des Eingriffs zu stellen sind. Dies hat zur Folge, dass Art. 9 DSGVO den Art. 6 DS-GVO nicht verdrängt, sondern dessen Voraussetzungen zusätzlich zu denen des Art. 6 DSGVO vorliegen müssen.

Automatisierte Entscheidungen, die auf Kategorien besonderer Daten beruhen, sind nur zulässig, wenn die betroffene Person ausdrücklich eingewilligt hat oder die Verarbeitung auf einer speziellen Rechtsgrundlage erfolgt und aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist (Art. 22 Abs. 4 DSGVO). Der Bundesgesetzgeber hat in § 37 Abs. 1 Nr. 2 BDSG eine solche Regelung zu Entscheidungen getroffen, die auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruhen. Soweit die Entscheidung auf der Verarbeitung von Gesundheitsdaten beruht, hat der Verantwortliche nach § 37 Abs. 2 BDSG angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 Satz 2 BDSG vorzusehen.

Verantwortliche, die besondere Datenkategorien verarbeiten, haben in jedem Fall ein Verzeichnis aller ihrer Zuständigkeit unterliegenden Verarbeitungstätigkeiten zu führen (Art. 30 Abs. 5 DSGVO). Im Falle einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten muss regelmäßig eine Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 Abs. 3 lit. b DSGVO).

Anforderungen an die datenverarbeitenden Personen

Grundsätzlich dürfen unter Beachtung der in Art. 9 Abs. 2 DSGVO genannten Voraussetzungen alle in Frage kommenden Personen die von Art. 9 Abs. 1 DSGVO erfassten Daten verarbeiten. Soweit derartige Daten allerdings zu den in Art. 9 Abs. 2 lit. h DSGVO genannten Zwecken (insbesondere Gesundheitsvorsorge und medizinische Versorgung) verarbeitet werden, legt Art. 9 Abs. 3 DSGVO spezifische Anforderungen an das Personal fest. Zwingende Voraussetzung für eine zulässige Verarbeitung ist dabei das Bestehen einer besonderen Geheimhaltungspflicht (Berufsgeheimnis oder Geheimhaltungsvorschrift), der die verarbeitende Person unterliegen muss.

10. Anlage 2 Ergänzende Regelungen

Regelungen die insbesondere die zur Realisierung der Datensicherheitsanforderungen des Art. 32 DSGVO zu treffende Maßnahmen betreffen sind im Besonderen:

- Verfahrensanweisung zur Erteilung von Auskünften
- Allgemeine Rahmendienstvereinbarung IT (ARDV-IT)
- DA Richtlinie zum sicheren Betrieb informationstechnischer Systeme (Betreiberrichtlinie)
- DV Videoüberwachung (DV-Video)
- DA Klassifizierung von Informationen
- Mitarbeitermerkblatt zum Umgang mit Passworten
- DV E-Mail und Internet
- DV Mobiles Arbeiten
-