Rahmenbetriebsvereinbarung für die Nutzung Mobiler Endgeräte und deren Verwaltung

(Mobile Devices Management)

Zwischen

Universitätsklinikum Heidelberg (im folgenden UKHD - Konzernleitung)

und

dem Konzernbetriebsrat des Universitätsklinikums Heidelberg (im folgenden KBR)

(Stand 31.05.2021)

*In dieser Betriebsvereinbarung wird die männliche Form für alle Geschlechter verwendet.

Inhaltsverzeichnis:

1. Präambel

Die Nutzung mobiler Geräte wie Smartphones und Tablets gewinnt immer mehr an Bedeutung. Neben dem Gebrauch als Kommunikationsmittel steht insbesondere die mobile Nutzung von betrieblichen Fachanwendungen im Fokus. Mit der Einführung von mobilen Endgeräten soll ein modernes Arbeitsumfeld geschaffen werden, welches auch zu Erhaltung und Weiterentwicklung von Arbeitsplätzen dienen soll.

Durch den Einsatz dieser Geräte können aber auch besondere Gefahren und Risiken, insbesondere in den Bereichen Datenschutz, Persönlichkeitsrechte sowie der IT-Sicherheit entstehen. Die mobile Arbeit darf weder die ständige Erreichbarkeit der Beschäftigten zum Ziel oder zu Folge haben noch eine Ausweitung des Arbeitsvolumens bewirken. Bei der Anwendung dieser Techniken wird der Datenschutz für alle Beschäftigten in jeder Hinsicht gewährleistet und die Beschäftigtenrechte nicht negativ berührt.

2. Zielsetzung

Diese Betriebsvereinbarung dient dem Schutz der Persönlichkeitsrechte der Beschäftigten und der Vermeidung von Datenmissbrauch und regelt die Nutzung von unternehmenseigenen mobilen Endgeräten oder von mobilen Endgeräten, die von einem Dritten mit eigentumsähnlichen Rechten zur Verfügung gestellt werden (z.B. Miete, Leasing) und der darauf gespeicherten Daten und angewendeten Applikationen, die den Beschäftigten als Arbeitsmittel zur Verfügung gestellt werden.

Der Einsatz von mobilen Endgeräten sowie eines Mobile Devices Management Systems soll neben der Wirtschaftlichkeit und Zweckmäßigkeit auch die Interessen der Beschäftigten berücksichtigen sowie die Rechte der Betriebsräte in den Tochtergesellschaften hierbei waren.

Die Nutzung von privaten Geräten der Beschäftigten im Unternehmensumfeld ist nicht Gegenstand dieser Vereinbarung.

3. Geltungsbereich

Diese Rahmenbetriebsvereinbarung gilt für alle Beschäftigten im Sinne des §5 BetrVG der jeweiligen Tochtergesellschaften des Universitätsklinikums Heidelberg, hierzu gehören auch die Beschäftigten des Universitätsklinikums Heidelberg und die Beschäftigten des Landes Baden-Württemberg, welche vom Universitätsklinikum Heidelberg in die Tochtergesellschaften gestellt werden.

Die mit der Umsetzung und Anwendung dieser Rahmenbetriebsvereinbarung beauftragten Dritten, z.B. Beschäftigte des Universitätsklinikums (Mitarbeiter des ZIM, Systemadministratoren, externe Firmen usw.) haben sich an die Vorgaben und Regularien dieser Rahmenbetriebsvereinbarung zu halten.

4. Begriffsbestimmungen/Klassifizierung

4.1 Mobile Device

Unter Mobile Device, im folgenden Mobilgerät, wird im Rahmen dieser Vereinbarung ein Endgerät verstanden, das ein Mobilgerätebetriebssystem – insbesondere Android und iOS – besitzt und über ein Mobile Device Management System (Konzern MDM-System) verwaltet werden kann. Dies sind insbesondere:

- Smartphones
- Tablets und ähnliche Bauformen
- spezielle Gerätebauformen mit einem Mobilgerätebetriebssystem

Nicht als Mobilgerät i.S. dieser Betriebsvereinbarung werden Geräte verstanden, die nicht über ein Mobile Device Management System (Konzern MDM-System) verwaltet werden können.

Die Mobilgeräte sind entsprechend dem vorgesehenen Verwendungszweck als Personal- oder Shared-Device klassifiziert und werden demensprechend konfiguriert. Dadurch soll sichergestellt werden, dass die Beschäftigten die Mobilgeräte entsprechend dem vorgesehenen Verwendungszweck einsetzen. Die konkrete Festlegung erfolgt im jeweiligen Anwendungsfall (Mobiler Use Case).

4.1.1 Shared Device

- Einer Personengruppe für spezifischen Zweck übergeben
- Nutzung als „Arbeitsmittel" in definierten betrieblichen Abläufen
- für definierten Einsatzzweck vorgesehen
- Technisch stark durch MDM reglementiert

4.1.2 Personal Device

- Einem Beschäftigten als persönliches Arbeitsmittel übergebenes Mobile Device
- Nutzung für Kommunikation und den Zugriff auf betriebliche Applikationen durch den Beschäftigten
- Beschäftigter nutzt Gerät entsprechend den eigenen Aufgaben und Bedarf
- MDM gibt Rahmen vor, innerhalb dessen das Gerät durch den Nutzer angepasst werden kann

4.2. Mobile Device Management System

Es wird ein Mobile Device Management System (Konzern MDM-System) als einheitliche IT-Plattform für die Verwaltung und Nutzung der Mobilgeräte und dessen Anwendungen eingesetzt. Die MDM-Administration nutzt das Konzern MDM-System als Verwaltungswerkzeug (z. B. Installation, Konfiguration, Betrieb) und stellt mobile Applikationen („Apps") und Netzwerkzugänge dem Nutzer bereit.

Das verwendete MDM-System und die System- Einstellungen sind im MDM-Systemsteckbrief spezifiziert (Anlage 1). Der KBR kann jederzeit die Übereinstimmung der Anlage 1 mit dem tatsächlichen System überprüfen.

Ein Austausch des Konzern MDM-Systems gegen ein anderes Produkt oder die Auslagerung an Dritte sowie Änderungen der im Systemsteckbrief definierten Einstellungen bedürfen der Zustimmung des KBR.

4.3 MDM-Administration

Welcher Dienstleister mit der MDM-Administration auf Konzernebene beauftragt wird, erfolgt in Abstimmung zwischen UKHD - Konzernleitung und Konzernbetriebsrat. UKHD - Konzernleitung und Konzernbetriebsrat sind sich zum Zeitpunkt der Unterzeichnung dieser Rahmenbetriebsvereinbarung einig, dass das Konzern-MDM-System als zentraler Standarddienst durch das Zentrum für Informations- und Medizintechnik betrieben wird.

Sollten in einem Tochterunternehmen der örtliche Betriebsrat und das Tochterunternehmen zu der Einschätzung kommen, dass für einen spezifischen Anwendungsfall („Mobiler Use Case") die in dieser Rahmenvereinbarung definierten Konzernstandards nicht die nötigen Anforderungen erfüllen, so können die beiden Parteien auf lokaler Ebene für den spezifischen Anwendungsfall eigenständige Regelungen vereinbaren.

4.4 Mobiler Use Cases

Unter einem Mobilen Use Case (Anwendungsfall) werden ein oder mehrere betriebliche Arbeitsprozesse verstanden, die mit Hilfe von mobilen Geräten und Anwendungen durchgeführt werden. Es erfolgt dabei ein Zugriff auf die Anwendungssysteme des UKHD oder der Tochterunternehmen und der darin gespeicherten Informationen und Daten.

5. Datenschutz

Es gilt die aktuelle Datenschutzgrundverordnung (DSGVO), insbesondere die Grundsätze nach §5 DSGVO zu der Verarbeitung personenbezogener Daten.

Die Daten werden ausschließlich für die in dieser Rahmenbetriebsvereinbarung vereinbarten Zwecke verwendet. Die Verarbeitung ist auf das erforderliche Mindestmaß beschränkt (Datenerforderlichkeit Datensparsamkeit, Zweckbindung, Verhältnismäßigkeit, Normenklarheit, siehe Anlage 1 Systemsteckbrief). Eine Datenspeicherung auf Vorrat ist unzulässig.

Benötigt ein Nutzer technischen Support, kann sich die MDM- Administration mithilfe einer betrieblich vorinstallierten App nach ausdrücklicher Erlaubnis durch die Beschäftigten auf das Mobilgerät aufschalten.

Für das MDM-System und den jeweiligen Use Case erfolgt eine Meldung zum Verarbeitungsverzeichnis sowie – sofern erforderlich – eine Datenschutzfolgeabschätzung, für den Fall der Verarbeitung personenbezogener Daten (gemäß DSGVO).

Eine Übermittlung von personenbezogenen Daten an Dritte findet grundsätzlich nicht statt, es sei denn die Datenübermittlung an Dritte ist über einen Use Case abgebildet.

Bei Auftragsdatenverarbeitung muss das UKHD den Auftragsnehmer im Dienstleitungsvertrag auf die Einhaltung der Bestimmungen dieser Rahmenbetriebsvereinbarung verpflichten. Verträge mit Dritten sind so zu gestalten, dass die Kontrolle des Konzernbetriebsrats auch gegenüber Dritten wahrgenommen werden können.

6. Rechte und Pflichten der Beschäftigten

Die Beschäftigten haben das Recht auf Einsicht und Erläuterung erfasster und ausgewerteter Daten, die ihre Person betreffen.

Keinesfalls dürfen Daten, die vom Beschäftigten eingegeben werden oder von Mobilgeräten, deren Anwendungen sowie dem MDM-System selbständig erstellt werden zur Leistungs- oder Verhaltenskontrolle sowie zu Überwachung der Beschäftigten eingesetzt und herangezogen werden. Sie unterliegen einem absoluten Beweisverwertungsverbot. Erfolgen Maßnahmen entgegen diesem Verbot, werden sie nach Aufforderung durch den betroffenen Beschäftigten oder durch den örtlichen Betriebsrat vom Arbeitgeber unverzüglich zurückgenommen.

Das Mobile Device Management System und der Einsatz der mobilen Endgeräte und den darauf installierten Anwendungen und Daten dürfen nicht zur Steigerung des Arbeits- und Leistungsdrucks der Beschäftigten führen.

Für technische Störungen in der Soft- und Hardware und der technischen Infrastruktur die das Arbeitsergebnis negativ beeinflussen sind die Beschäftigten nicht in die Verantwortung zu ziehen bzw. haftbar zu machen.

Die Beschäftigten haften bei einem grob fahrlässigen oder vorsätzlichen Verstoß gegen diese Rahmenbetriebsvereinbarung und Schäden, die dem Konzern oder einem Dritten entstehen.

7. Schulungs- Qualifizierungs- und Informationsmaßnahmen

Beim Einsatz von mobilen Endgeräten für betriebliche Zwecke hat das Tochterunternehmen dafür Sorge zu tragen, dass die betroffenen Beschäftigten über die notwendigen Kenntnisse zur Nutzung der Geräte und der darauf installierten Applikationen verfügen.

Dies umfasst zum einen die allgemeinen - Use-Case-unabhängigen - Informationen und Regelungen:

- diese Rahmenbetriebsvereinbarung
- allgemeine Nutzungsrichtlinie
- "Privacy"-Einstellungen des Mobile Device Management (erfasste Daten und Berechtigungen)
- Anwenderdokumentation für Personal-Devices ("Diensthandys")

Diese Dokumente werden allen Beschäftigten im Intranet sowie bei der Bereitstellung eines Gerätes zur Verfügung gestellt.

Des Weiteren sind bei der Einführung eines jeden Use Case vor der erstmaligen Bereitstellung von Mobilgeräten die Beschäftigten in geeigneter Weise umfassend in die genutzten Gerätefunktionen und Applikationen einzuweisen.

Wann, wie und welche Schulungs- und Qualifizierungsmaßnahmen in den jeweiligen Tochterunternehmen durchgeführt werden, erfolgt Use-Case-spezifisch in Abstimmung mit den örtlichen Betriebsräten. Dazu gehören z.B.

- erforderliche Schulungsunterlagen
- erforderliche Schulungsmaßnahmen
- Bereitstellung von Bedienungsanleitungen und ggfls. Benutzerhandbüchern

Darüber hinaus wird sichergestellt, dass die Beschäftigten unter Berücksichtigung der betrieblichen Möglichkeiten, persönlicher Fähigkeiten und wirtschaftlicher Zweckmäßigkeit für die vorgesehene Nutzung und den übertragenen Aufgaben die jeweils erforderliche Unterstützung erhalten.

Die Schulungs- und Qualifizierungsmaßnahmen haben während der Arbeitszeit stattzufinden, die Kosten hierfür trägt das Tochterunternehmen.

8. Zuständigkeiten: Beteiligungsrechte der örtlichen Betriebsräte und des KBR

Jede Einführung von mobilen Endgeräten, Use-Cases und Applikationen und ggfls. eines alternativen MDM-Systems in einem Tochterunternehmen unterliegt der Mitbestimmung des jeweiligen örtlichen Betriebsrates, dieses umfasst auch die Pilotierung und den Testbetrieb oder die Änderung von bereits eingeführten mobilen Endgeräten, Use-Cases und Applikationen.

8.1 Mobile Endgeräte

Die Festlegung der für den Unternehmenseinsatz im Tochterunternehmen unterstützten Endgerätemodelle, Zubehör und Software erfolgt durch die jeweilige Geschäftsführung unter Beteiligung der MDM-Administration und unter Berücksichtigung der Funktionalität, technischen Eignung sowie Anschaffungs- und Betriebskosten. Die Verwendung eines bestimmten Gerätemodells für einen bestimmten Einsatzzweck unterliegt der Mitbestimmung des örtlichen Betriebsrates.

8.2 MDM-System

Das verwendete Konzern MDM-System unterliegt der Mitbestimmung des Konzernbetriebsrates. Die jeweiligen Systemeinstellungen (Berechtigungskonzept) sind in einem MDM-Systemsteckbrief (Anlage 1) spezifiziert.

Der Konzernbetriebsrat kann jederzeit die Übereinstimmung der mitbestimmten Vorgaben des Systemsteckbriefs mit dem tatsächlichen System überprüfen.

Ein Austausch des Konzern MDM-Systems gegen ein anderes Produkt oder die Auslagerung an Dritte sowie Änderungen der im Systemsteckbrief definierten Einstellungen oder Updates, die

Änderungen des Systemsteckbriefs zur Folge haben, bedürfen der Zustimmung des Konzernbetriebsrates.

8.3 Use Case

Bei der Einführung oder Änderung von Anwendungsfällen ist wie folgt zu verfahren:

Das Tochterunternehmen informiert den jeweiligen örtlichen Betriebsrat darüber, dass ein (neuer) Anwendungsfall eingeführt bzw. geändert werden soll. Unter Beteiligung des örtlichen Betriebsrates und des Datenschutzbeauftragten erstellt das Tochterunternehmen eine schriftliche Dokumentation zu dem Anwendungsfall. Die Dokumentation beinhaltet das Nutzungsszenario, die Festlegung welches mobile Endgerät eingesetzt werden soll, die Festlegung ob Shared-Device oder Personal-Device, Schnittstellen, Zielsystem/-daten, Einstellungen, betroffene Personengruppe, MDM-Administration, Support/Wartung, Rechtekonzept etc.

Diese Dokumentation wird dem örtlichen Betriebsrat zur Mitbestimmung vorgelegt, ggf. werden Regelungen für den Anwendungsfall über eine Betriebsvereinbarung auf lokaler Ebene getroffen.

9. Kontrollrechte des Konzernbetriebsrates und der örtlichen BR

Der Konzernbetriebsrat und die örtlichen Betriebsräte haben das Recht, jederzeit die Einhaltung dieser Rahmenbetriebsvereinbarung zu kontrollieren.

Bei der Einführung eines Use Case sind die zur Ausübung der Kontrollrechte zusätzlich benötigten Prüfhilfen, Programme, Dokumentationen oder Berichte im Rahmen des Mitbestimmungsverfahrens mit dem örtlichen BR festzulegen und zu erstellen. Der örtliche Betriebsrat kann nach Zustimmung der jeweiligen Geschäftsführung zur Durchführung dieser Aufgaben einen Sachverständigen seiner Wahl hinzuziehen.

Die Beschäftigten haben das Recht und die Pflicht dem örtlichen Betriebsrat oder dem Konzernbetriebsrat gewünschte Auskünfte zur Funktionsweise der mobilen Endgeräte, des MDM-Systems oder den bereitgestellten Applikationen zu geben. Der Dienstleister für die MDM – Administration bzw. die jeweilige betriebsinterne DV-Administration sind dem örtlichen Betriebsrat und dem Konzernbetriebsrat zu Auskünften über Systeminhalte und deren Anwendungen verpflichtet.

10. Nutzung der Mobilen Endgeräte (Shared Device und Personal Device)

10.1 Betriebliche Nutzung

Das Tochterunternehmen stellt den Beschäftigten ein Mobilgerät zur Erbringung der Arbeitsleistung zur Verfügung auf der Grundlage eines oder mehrere Use-Cases.

Die für die betriebliche Nutzung erforderlichen Apps der Shared Devices und der Personal Devices werden ausschließlich durch die MDM-Administration bereitgestellt und sind abschließend im Use Case definiert. Die Mobilgeräte sind bei Bedarf je nach den Anforderungen eines Use Cases mit einer SIM-Karte eines Mobilfunkanbieters ausgestattet.

Die Mobilgeräte dürfen ausschließlich von Beschäftigten und nicht von Dritten benutzt werden, es sei denn der Use Case sieht die Nutzung ausdrücklich vor.

Das Tochterunternehmen übernimmt sämtliche mit der betrieblichen Nutzung in Verbindung stehenden Kosten und Versicherungen inclusive aller Hilfsmittel, die das Gerät schützen. Das Tochterunternehmen stellt einen Ort zur Verfügung an dem die mobilen Endgeräte sicher und betriebsbereit verwahrt werden.

10.2 Private Nutzung

Eine private Nutzung von Shared Devices ist nicht gestattet. Die Geräte sind ausschließlich für die im Use Case definierten Aufgaben zu verwenden.

Die private Nutzung (Telefonie, E-Mail und Internet) der Mobilgeräte (Personal Devices) während der Arbeitszeit ist im geringfügigen Umfang zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden.

Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch ist unzulässig.

Im Rahmen der privaten Nutzung dürfen keine kommerziell - gewerblichen, freiberuflichen oder sonstigen geschäftlichen Zwecke verfolgt werden.

Eine private Nutzung der Mobilgeräte (Personal Devices) in der Freizeit (mit Nutzungspauschale) ist nicht vorgesehen.

10.3 Übergangsregelung für die „Option der privaten Nutzung von mobilen Endgeräten in der Freizeit (Nutzungspauschale)“

Für die Beschäftigten beim Universitätsklinikum Heidelberg besteht die Möglichkeit, dass persönlich zugeordnete Mobilgeräte (Personal Devices) von den Beschäftigten auch für private Zwecke (z. B. Telefonie, Internet) verwendet werden dürfen, gegen eine Nutzungspausschale. Dieses Angebot wird teilweise auch von Beschäftigten der Tochterunternehmen des Universitätsklinikums Heidelberg in Anspruch genommen.

Im Zuge des Datenschutzes, des Arbeits- und Gesundheitsschutzes sowie des Haftungsrechtes, wird ab Einführung dieser Rahmenbetriebsvereinbarung die „Option der privaten Nutzung von mobilen Geräten in der Freizeit (Nutzungspauschale)“ den Beschäftigten der Tochtergesellschaften nicht mehr zur Verfügung stehen.

Beschäftigte welche bereits diese Option in Anspruch nehmen, bleibt diese auch nach Einführung dieser Rahmenbetriebsvereinbarung bis zum nächsten Gerätewechsel erhalten.

Diese Beschäftigten sind umgehend über die datenschutzrechtlichen Gefahren, zu Haftungsfragen sowie zum Arbeits- und Gesundheitsschutz gesondert schriftlich aufzuklären. Die Beschäftigten bestätigten dieses mit ihrer Unterschrift.

11. Datenverarbeitung / Datenspeicherung

Die Daten des Konzern MDM-Systems (z. B. Geräte- und Benutzerinformationen) sind auf den Servern des Universitätsklinikums Heidelbergzentral gespeichert. Im Falle einer Datenspeicherung – und Verarbeitung bei Drittanbietern muss dieses in Deutschland geschehen.

Der Speicherort der Daten des Konzern MDM-Systems ist dem MDM-Systemsteckbrief (Anlage 1) spezifiziert. Eine Änderung bedarf der Zustimmung des Konzernbetriebsrates.

Die Verarbeitung und Speicherung der in einem Use Case nach dieser Vereinbarung erhobenen Daten sind den Dokumentationen und Regelungen zu den einzelnen Use Cases zu entnehmen.

Die für die betriebliche Nutzung (Use-Case) erforderlichen Apps der Shared-Devices und der Personal Devices sind abschließend in den jeweiligen Use Cases definiert und werden ausschließlich durch das MDM-System bereitgestellt.

Für Shared Devices ist weitestgehend technisch sichergestellt, dass Beschäftigte keine Apps hinzufügen oder installierte Apps entfernen können. Die Beschäftigten sind ungeachtet dessen nicht berechtigt, einem Shared Device Apps hinzuzufügen oder installierte Apps zu entfernen.

Bei Personal Devices lässt das MDM-System die Installation und Deinstallation von Apps zu, damit Beschäftigte das Gerät nach eigenem Bedarf anpassen können. Zulässig ist jedoch nur die Nutzung von Apps für betriebliche Zwecke oder im Rahmen der Privatnutzung in geringem Umfang.

Hierfür dürfen nur der auf dem Endgerät bereits vorhandene offizielle Geräte-App-Store (z. B. Apple Store) und der konzerneigene -Unternehmens-App-Store genutzt werden. Das Hinzufügen zusätzlicher App-Stores oder die Installation von Apps unter Umgehung der genannten Standard-App-Stores ist nicht gestattet.

12. Datensicherheit

12.1 Backup und Wiederherstellung

Es erfolgt kein Backup und keine Wiederherstellung der lokal auf dem Gerät gespeicherten Daten. Für betriebliche Daten und Anwendungen achtet das Tochterunternehmen darauf, dass durch technische oder organisatorische Maßnahmen sichergestellt ist, dass eine Datensicherung auf den zentralen Servern erfolgt. Ob und wie eine Datensicherung erfolgt, ergibt sich aus den jeweiligen Use-Cases.

In einem Wiederherstellungsfall erfolgt eine Neuinstallation.

12.2 Sicherheits- und Datenschutzvorfall

Besteht ein durch Tatsachen begründeter Verdacht, dass ein Beschäftigter das Mobilgerät oder das MDM-System missbräuchlich oder unerlaubt nutzt, insbesondere gegen seine Verpflichtungen aus Ziffer 6 dieser Vereinbarung verstößt (Datenschutzvorfall), sind einzuleitende Maßnahmen mit dem örtlichen Betriebsrat zu vereinbaren. Falls erforderlich kann das Mobilgerät von der MDM-Administration gesperrt werden, so dass eine Nutzung nicht mehr möglich ist.

Ein Sicherheits- oder Datenschutzvorfall ist ebenfalls gegeben, wenn ein begründeter Verdacht besteht, dass ein Mobilgerät verloren gegangen ist, gestohlen wurde, ein unberechtigter Zugang bzw. Zugriff besteht, es mit Schad-Software verseucht wurde oder Daten auf dem Mobilgerät manipuliert wurden.

Das Tochterunternehmen hat der MDM-Administration, den Beauftragten für Informationssicherheit und den Beauftragten für Datenschutz und dem örtlichen Betriebsrat die erforderlichen Informationen zu den Vorfällen zu übermitteln und zu unterstützen.

12.3 Datenlöschung

Das Tochterunternehmen ist berechtigt - durch die MDM-Administration- jederzeit alle Informationen und Daten auf einem Mobilgerät, das als Shared Device und Personal Device genutzt wird, zu löschen.

Sollen Informationen und Daten eines Mobilgeräts, das als Personal Device genutzt wird, gelöscht werden (Besitzerwechsel, Neuinstallation, usw.), informiert die MDM-Administration die Beschäftigten zunächst rechtzeitig über die beabsichtigte Löschung und gibt ihnen die Gelegenheit, innerhalb einer Frist von zwei Monaten die Daten der Privatnutzung zu sichern bzw. selbst zu löschen.

Bei Besitzerwechsel sorgt die MDM-Administration dafür, dass eventuell noch vorhandene Daten vor der Weitergabe des Gerätes gelöscht werden z.B. im Zuge der Neuinstallation.

Hierzu informiert das Tochterunternehmen die MDM-Administration rechtzeitig über den personellen Wechsel bzw. das Ausscheiden der Beschäftigten.

Bei einem Sicherheitsvorfall ist die MDM-Administration berechtigt, eine unverzügliche Löschung der Informationen und Daten auf dem Mobilgerät vorzunehmen. Die Beschäftigten sind von der MDM-Administration in Kenntnis zu setzen.

13. Arbeits- und Gesundheitsschutz

Das Tochterunternehmen ist im Hinblick auf den jeweiligen Use Case verpflichtet, alle erforderlichen Arbeitsschutzmaßnahmen unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen (§3 abs. 1 ArbSchG). Das bedeutet zum

Beispiel, dass für mobiles Arbeiten die Ausstattung mit Arbeitsgeräten, die eine ergonomische Arbeit ermöglichen, gewährleistet ist

13.1. Gefährdungsbeurteilung

Das Tochterunternehmen muss auch für mobile Arbeit eine Gefährdungsbeurteilung durchführen (§5 Abs. 1 ArbSchG) und deren Ergebnisse dokumentieren (§6 Abs.1 ArbSchG). Dabei hat das Tochterunternehmen zu prüfen, unter welchen Umständen mobile Arbeit tatsächlich stattfindet.

Bestehende Betriebsvereinbarungen in den einzelnen Tochtergesellschaften haben hierbei Anwendung zu finden.

13.2 Arbeitsmedizinische Vorsorge

Das Tochterunternehmen hat auf der Grundlage der Gefährdungsbeurteilung für eine angemessene arbeitsmedizinische Vorsorge zu sorgen. Dabei hat es die Vorschriften der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) umzusetzen.

Demnach hat das Tochterunternehmen Beschäftigten, die Tätigkeiten z.B. an Bildschirmgeräten durchführen eine Angebotsvorsorge anzubieten.

Diese Angebotsvorsorge enthält das Angebot auf eine angemessene Untersuchung der Augen und des Sehvermögens. Erweist sich auf Grund der Angebotsvorsorge eine augenärztliche Untersuchung als erforderlich, so ist diese zu ermöglichen, dieses gilt entsprechend für Sehbeschwerden.

Den Beschäftigten sind im erforderlichen Umfang spezielle Sehhilfen für ihre Arbeit an Bildschirmgeräten zur Verfügung zu stellen, wenn es ein Ergebnis der Angebotsvorsorge ist, dass spezielle Sehhilfen notwendig und normale Sehhilfen nicht geeignet sind.

Bestehende Betriebsvereinbarungen in den einzelnen Tochtergesellschaften haben hierbei Anwendung zu finden.

13.3 Arbeitszeit, Erreichbarkeit und Ruhezeiten

Die geltenden Arbeitszeitregelungen im Arbeitszeitgesetz, in Tarifverträgen, sowie in den bestehenden Betriebsvereinbarungen bleiben weiterhin vollumfänglich in Kraft.

Eine Erweiterung des Arbeitsvolumens durch den Einsatz von Mobilgeräten ist ausdrücklich nicht vorgesehen. Dem Arbeitgeber und den Betriebsräten ist bewusst, dass mobiles Arbeiten ein hohes Risiko der Entgrenzung der Arbeit bedeutet. Auf das Einhalten der geltenden Arbeitszeitregelungen ist vom Beschäftigten, vom Tochterunternehmen bzw. vom jeweiligen Vorgesetzten zu achten.

Die betriebliche Nutzung des Mobilgerätes erfolgt daher grundsätzlich nur innerhalb der jeweils tariflichen-, arbeitsvertraglichen- und betrieblich geltenden Arbeitszeitregelungen.

Arbeitszeiten im Sinne dieser Regelung sind auch Bereitschafts- und Rufbereitschaftszeiten. Das Bereithalten eines Mobilgerätes außerhalb der Arbeitszeit darf vom Arbeitgeber nicht angeordnet werden.

14. Meinungsverschiedenheiten

Meinungsverschiedenheiten und Streitigkeiten aller sich aus dieser Rahmenbetriebsvereinbarung ergebenden Streitfragen in den Tochterunternehmen sind zunächst in einem internen Gespräch zwischen Tochterunternehmen und örtlichen Betriebsrat – falls erforderlich unter Hinzuziehung des Konzernbetriebsrats - mit dem ernsthaften Willen zur Einigung und unter Nennung des konkreten Streitpunktes zu klären. Kommt es zu keiner internen Einigung, ist die Einigungsstelle mit je 3 Beisitzern pro Seite anzurufen.

15. Inkrafttreten / Kündigung / Schlussbestimmungen

Diese Rahmenbetriebsvereinbarung tritt am Tag der Unterzeichnung in Kraft. Sie kann mit einer Frist von 6 Monaten zum Ende eines Kalenderjahres von jeder Seite erstmalig zum 31.12.2022 gekündigt werden, wirkt aber solange nach bis eine neue Rahmenbetriebsvereinbarung abgeschlossen ist.

Die Anlagen sind separat jederzeit mit einer Frist von einem Monat zum Monatsende kündbar.

Im gegenseitigen Einvernehmen kann diese Rahmenbetriebsvereinbarung unabhängig von einer Kündigung angepasst werden.

Heidelberg, den 31.05.2021

Für das Universitätsklinikums Heidelberg (Konzernleitung)

Prof. Dr. Ingo Autenrieth
(Leitender Ärztlicher Direktor - Vorstandsvorsitzender UKHD)

Für den Konzernbetriebsrat der Tochtergesellschaften

Stefan Michael
(Vorsitzender des Konzernbetriebsrats)

Anlagenverzeichnis

Anlage 1 – Muster Systemsteckbrief Mobile Devices - MDM
Anlage 2 – Nutzungsrichtlinie für Anwender