UNIVERSITÄTS
KLINIKUM
HEIDELBERG

Dienstvereinbarung Mobile Devices

Zwischen

dem UNIVERSITÄTSKLINIKUM HEIDELBERG, Anstalt des öffentlichen Rechts,
im folgenden UK,

und

dem PERSONALRAT DES UNIVERSITÄTSKLINIKUMS HEIDELBERG,
im folgenden PR

wird folgende

DIENSTVEREINBARUNG gemäß §§ 75 Absatz 4 Nummer 16, 85 Landespersonalvertretungsgesetz für Baden-Württemberg zur Regelungen des Einsatzes von unternehmenseigenen mobilen Endgeräten und Applikationen am Universitätsklinikum Heidelberg (**DV Mobile Devices**) geschlossen:

Präambel

Die Nutzung mobiler Geräte wie Smartphones und Tablets gewinnt immer mehr an Bedeutung. Neben dem Gebrauch als Kommunikationsmittel steht im UK insbesondere die flexible Nutzung von klinischen und betrieblichen Fachanwendungen im Fokus.

Die Parteien wollen Chancen nutzen, die sich aufgrund mobiler Geräte ergeben, und ein modernes Arbeitsumfeld bieten. Gleichzeitig ergeben sich durch den Einsatz dieser Geräte besondere Gefahren und Risiken, insbesondere in den Bereichen Persönlichkeits- und Datenschutz sowie der IT-Sicherheit. Bei den Parteien besteht daher Einigkeit, dass der Schutz von Informationen und Daten einschließlich der Vertraulichkeit des gesprochenen Wortes sowie die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität elektronisch verarbeiteter Informationen und Daten gewährleistet ist. Keinesfalls dürfen

Mobilgeräte, ihre Anwendungen und Verwaltungswerkzeuge zur Leistungs- oder Verhaltenskontrolle der Beschäftigten eingesetzt werden.

I Grundlagen

Diese Dienstvereinbarung regelt die Nutzung von Geräten, die im Eigentum des UK stehen oder dem UK von einem Dritten mit eigentumsähnlichen Rechten zur Verfügung gestellt sind (Miete, Leasing) und den Beschäftigten als Arbeitsmittel zur Verfügung gestellt werden. Die Nutzung von privaten Geräten der Beschäftigten im Unternehmensumfeld ist nicht Gegenstand dieser Vereinbarung.

In diesem Zusammenhang ist diese Dienstvereinbarung die Grundlage für die Verarbeitung von personenbezogenen Beschäftigtendaten gemäß der Datenschutzgrundverordnung (DSGVO).

II Geltungsbereich

Diese Dienstvereinbarung gilt für alle in einem Beschäftigungsverhältnis, Dienstverhältnis oder einem Ausbildungsverhältnis zum Universitätsklinikum Heidelberg stehende Beschäftigte, Auszubildende und sonstige Beschäftigte im Sinne des § 4 Absatz 1 und 2 LPVG sowie die am Universitätsklinikum tätigen Landesbeschäftigten (im folgenden „Beschäftigte")

Die Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz vom 13.05.2011 in der Fassung vom 09.01.2017 (im Folgenden „DV Internet/ E-Mail") wird durch diese Regelungen nicht berührt.

III Definitionen

1. Mobile Devices

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 verwaltet werden kann. Dies sind insbesondere:

- Smartphones
- Tablets und ähnliche Bauformen
- Spezielle Gerätebauformen mit einem Mobilgerätebetriebssystem wie z. B. intelligente Barcode Scanner

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

2. Mobile Device Management System

Am UK wird ein *Mobile Device Management System* (MDM-System) als einheitliche IT-Plattform für die Verwaltung und Nutzung der Mobilgeräte und Anwendungen eingesetzt. Das MDM-System dient der MDM-Administration als Verwaltungswerkzeug (z. B. Installation, Konfiguration, Betrieb) und stellt Beschäftigten mobile Applikationen („Apps") und Netzwerkzugänge bereit.

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

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

Der Zugang und die Berechtigung auf die administrative Oberfläche des MDM-Systems sind im Systemsteckbrief **(Anlage 1)** definiert.

Eine Kontrolle des Verhaltens und der Leistung der Beschäftigten ist ausgeschlossen.

Bei begründetem Verdacht auf missbräuchliche bzw. unerlaubte Nutzung des Mobilgerätes sind die gemäß Anlage 1 definierten MDM-Administratoren nach Zustimmung durch den PR zu einer Missbrauchskontrolle nach Ziffer IV.3 dieser Vereinbarung i.V.m. § 8 der DV Internet /E-Mail berechtigt.

3. Geräteklassifizierung

Diese Vereinbarung regelt die folgende Geräteklassifizierung eines Mobilgerätes:

Geräteklassifizierung	
„Shared Device"	**„Personal Device"**
einer Personengruppe für spezifischen Zweck übergeben.	einem Mitarbeiter zur persönlichen Nutzung übergeben
Nutzung als „Arbeitsmittel" in definierten betrieblichen Abläufen z. B. im klinischen Betrieb	Nutzung für Kommunikation und den Zugriff auf betriebliche Applikationen durch den Mitarbeiter
für definierten Einsatzzweck vorgesehen (teilweise auch kritische Dienste)	Mitarbeiter nutzt Gerät entsprechend den eigenen Aufgaben und Bedarf
technisch stark durch MDM reglementiert	MDM gibt Rahmen vor, innerhalb dessen das Gerät durch den Nutzer angepasst werden kann

Die Mobilgeräte sind entsprechend dem vorgesehenen Verwendungszweck als Personal- oder Shared-Device konfiguriert. Durch diese Konfiguration ist weitestgehend sichergestellt, dass die

Beschäftigten die Mobilgeräte entsprechend dem vorgesehenen Verwendungszweck einsetzen.

Ungeachtet dessen sind Beschäftigte grundsätzlich nicht berechtigt, Mobilgeräte über den vorgesehenen Verwendungszweck hinaus einzusetzen.

4. Mobiler Use Case

Unter einem Mobilen Use Case (Anwendungsfall) wird ein einzelner betrieblicher Arbeitsprozess verstanden, der mit Hilfe von mobilen Geräten und Anwendungen durchgeführt wird. Es erfolgt dabei ein Zugriff auf die Anwendungssysteme des UK und dort gespeicherte Informationen und Daten.

Jede Einführung (umfasst auch die Pilotierung und den Testbetrieb) oder Änderung von Anwendungsfällen unterliegt der Mitbestimmung des PR.

Bei der Einführung oder Änderung von Anwendungsfällen ist wie folgt zu verfahren: Die anfordernde Fachabteilung erstellt in Zusammenarbeit mit der MDM-Administration und unter Beteiligung der Datenschutzbeauftragten und der Informationssicherheit eine schriftliche Dokumentation mit den Eckdaten (z. B. Nutzungsszenario Shared/Personal-Device, Zielsystem/-daten, Einstellungen, betroffene Personengruppe etc.). Diese Dokumentation wird dem PR zur Mitbestimmung vorgelegt.

IV Mobilgerät

1.Bereitstellung des Mobilgeräts

Das UK stellt durch die MDM-Administration Beschäftigten ein Mobilgerät zur Erbringung der Arbeitsleistung nach Antragsstellung unter Vorlage des Mobile Device-Antragsformular **(Anlage 2)** zur Verfügung.

Die Mobilgeräte sind je nach Voraussetzung eines Use Cases mit einer SIM-Karte eines Mobilfunkanbieters für das UK ausgestattet.

Die verwendeten und unterstützen Gerätemodelle, Plattformen und das Zubehör werden ausschließlich durch die MDM-Administration festgelegt und installiert.

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

Das UK übernimmt sämtliche mit der betrieblichen Nutzung in Verbindung stehenden Kosten und Versicherungen inclusive aller Hilfsmittel, die das Gerät schützen (UK gibt den Warenkorb vor).

Die Beschäftigten haften für Schäden des UK wegen des Verlusts oder der Beschädigung des Mobilgeräts nur im Falle grober Fahrlässigkeit oder Vorsatz.

2.Datenverarbeitung und Konfiguration der Mobilgeräte

a) Datenverarbeitung

Die Daten des MDM-Systems (z. B. Geräte- und Benutzerinformationen) sind auf den Servern des UK zentral gespeichert. Die durch das MDM auf dem Gerät erfassten Daten und die dafür notwendigen MDM-Systemeinstellungen sind im MDM-Systemsteckbrief **(Anlage 1)** im Kapitel „Privacy" dokumentiert.

Die Verarbeitung der in einem Use Case nach III.4 dieser Vereinbarung erhobenen Daten bleibt – unter Berücksichtigung der Mitbestimmung des PR - den Regelungen der Parteien für den einzelnen Use Case vorbehalten.

b) Installierte Anwendungen (Apps)

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.

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

Im Falle einer Privatnutzung eines Personal Devices gemäß V.3 dieser Vereinbarung sind die Beschäftigten berechtigt, eigene Apps hinzuzufügen oder zu entfernen. Hierfür dürfen nur der auf dem Endgerät bereits vorhandene offizielle Geräte-App-Store (z. B. Apple Store) und der UK-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.

Das UK ist berechtigt spezifische Apps oder einzelne App-Funktionen (z. B. Zugriff auf Unternehmenskontakte) auf Unternehmensgeräten zu verbieten, wenn diese z. B. der betrieblichen Nutzung oder Interessen der Informationssicherheit oder des Datenschutzes widersprechen. In diesem Fall wird die App zentral im MDM-System gesperrt, so dass eine Nutzung auf dem Unternehmensgerät nicht möglich ist.

Die Beschäftigten haften im Verhältnis zum Anbieter einer für die Privatnutzung installierten App persönlich für die Einhaltung der Vertrags- und Lizenzbedingungen und verpflichten sich, das UK von Ansprüchen Dritter aus der Privatnutzung freizustellen.

c) Backup und Wiederherstellung

Es erfolgt kein Backup und keine Wiederherstellung der lokal auf dem Gerät gespeicherten Daten auf den Mobilgeräten. Für betriebliche Anwendungen achtet das UK darauf, dass durch technische oder organisatorische Maßnahmen sichergestellt ist, dass die Datenspeicherung auf den zentralen Servern erfolgt.

Für das Backup und die Wiederherstellung von Daten der Privatnutzung sind die Beschäftigten im eigenen Interesse verantwortlich. In einem Wiederherstellungsfall erfolgt eine Neuinstallation.

3.Sperren von Mobilgeräten und Sicherheits-/Datenschutzvorfall

Das UK ist berechtigt durch die Support-Administration, das Mobilgerät kurzfristig nach eigenem technischem Ermessen zu sperren, so dass eine Nutzung nicht mehr möglich ist, insbesondere wenn der begründete Verdacht besteht, dass das Mobilgerät von den Beschäftigten unter Verstoß gegen die Nutzungsrichtlinie verwendet wird oder wenn ein Sicherheits- oder Datenschutzvorfall vorliegt.

Ein Sicherheits- oder Datenschutzvorfall ist gegeben, wenn ein begründeter Verdacht besteht, dass ein Mobilgerät gestohlen wurde, ein unberechtigter Zugang besteht/erfolgt, ein unberechtigter Zugriff auf Daten besteht/erfolgt, es kompromittiert oder verloren gegangen ist, es mit Schadsoftware verseucht oder die Nutzung aus sonstigen Gründen unsicher ist. Ein Datenschutzvorfall liegt außerdem vor, wenn im Rahmen eines Use Case von einem konkreten Risiko für die von Datenverarbeitung oder Kommunikation betroffenen Beschäftigten auszugehen ist.

Die Beschäftigten sind von der Support-Administration über die Sperrung in Kenntnis zu setzen. Die Support-Administration hat den Beauftragten für Informationssicherheit und den Beauftragten für Datenschutz die erforderlichen Informationen zu Vorfällen zu übermitteln.

4.Löschen von Mobilgeräten

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

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

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

V Nutzung

1.Nutzung der Mobilgeräte und Haftung

Die Beschäftigten verpflichten sich, jede Nutzung zu unterlassen, die gegen diese Dienstvereinbarung, gegen die Mobile Device Nutzungsrichtlinie **(Anlage 3)** oder gegen sonstiges geltendes Recht verstößt oder die geeignet ist die Sicherheit der IT-Struktur zu beeinträchtigen oder im Rahmen eines Use Case Risiken für Betroffene der Verarbeitung bzw. Kommunikation hervorruft.

Die Beschäftigten haften bei einem grob fahrlässigen oder vorsätzlichen Verstoß für Schäden, die dem UK oder einem Dritten entstehen.

Das UK behält sich arbeitsrechtliche oder disziplinarische Schritte unter Beachtung der Mitbestimmungsrechte des PR vor.

Wird ein Mobilgerät ausschließlich als Shared Device genutzt, sind für die Einhaltung der o.g. Verpflichtungen dieser Dienstvereinbarung die jeweils aktuell das Mobilgerät nutzenden Beschäftigten und der Antragssteller nach IV. 1 dieser Vereinbarung verantwortlich.

2.Betriebliche Nutzung - Arbeitszeit

Die betriebliche Nutzung des Mobilgeräts erfolgt grundsätzlich nur innerhalb der vertraglichen Arbeitszeit der Beschäftigten. Arbeitszeit im Sinne dieser Regelung sind auch Bereitschafts- und Rufbereitschaftszeiten. Das Bereithalten eines Mobilgeräts außerhalb der Arbeitszeit darf vom UK nicht angeordnet werden.

3. Privatnutzung - Freizeit

Eine Nutzung von Shared Devices während der Freizeit ist nicht gestattet. Die Geräte sind ausschließlich für die im Use Case definierten Aufgaben zu verwenden (s. III.3).

Mobilgeräte mit einer Nutzung als Personal Device dürfen von den Beschäftigten während der Arbeitszeit im Rahmen der Regelungen der DV Internet/ E-Mail privat genutzt werden. Eine darüber hinausgehende private Nutzung (Privatnutzung), ist nur zulässig, wenn die Beschäftigten dazu eine Erklärung

zur Privatnutzung (Zahlung einer Nutzungspauschale) bei der Beantragung abgegeben haben und das UK diese annimmt.

Die Privatnutzung (bei Zahlung einer Nutzungspauschale) ist eine freiwillige Leistung des UK. Im begründeten Einzelfall kann einseitig die Privatnutzung mit einer Ankündigungsfrist von 6 Wochen zum Ende eines Kalendermonats widerrufen werden.

Die Privatnutzung darf keine Kosten verursachen, die die vereinbarte Nutzungspauschale übersteigen. Eine darüber hinausgehende Nutzung berechtigt das Universitätsklinikum zum sofortigen Entzug der Privatnutzung.

Die Kosten der zur Privatnutzung installierten Apps gemäß IV.2b und etwaige weitere bei der Privatnutzung anfallende Kosten tragen die Beschäftigten. Die aktuellen Tarifbedingungen sind im Intranet veröffentlicht.

Das UK behält sich vor die Installation für einzelne Apps zu untersagen, wenn diese den Belangen der Informationssicherheit, des Datenschutzes oder der betrieblichen Nutzung (z. B. Inkompatibilität mit Unternehmens-Apps) widersprechen.

Das UK stellt sicher, dass keine Aufzeichnung der Nutzungsdaten der zur Privatnutzung installierten Apps und kein Zugriff auf diese Daten erfolgt.

Sollte den Beschäftigten bei der Privatnutzung des Mobilgeräts ein Schaden, wie z.B. ein Verlust privater Daten entstehen, haftet das UK nur bei vorsätzlichem oder grob fahrlässigem Handeln seiner MDM bzw. Support Administration.

VI Personenbezogene Daten /Datenschutz

Für die im MDM-System gespeicherten Daten der Anlage 1 zur zweckgebundenen Verwendung gelten die in der Anlage 1 unter III.1. geregelten Einstellungen und administrativen Befehle.

Das MDM- System speichert die in der Anlage 1 unter III.3. genannten personenbezogenen Daten. Es ist im Hinblick auf weitere Daten, die über die in der Anlage 1 genannten Daten hinaus gehen, im Sinne der Datensparsamkeit so konfiguriert, dass nur so viele personenbezogene Daten gesammelt und aufbewahrt werden, wie es für den jeweiligen Use Case unbedingt notwendig ist. Hierüber werden für den jeweiligen Use Case im Rahmen der kollektivrechtlichen Beteiligung des PR gesonderte Regelungen vereinbart.

Das MDM-System verarbeitet keine Anwendungsdaten der installierten Apps.

Jedes Mitschneiden oder das Zugreifen auf Tonnachrichten oder die persönliche Kommunikation der Beschäftigten (z. B. E-Mail) ist technisch durch das MDM-System nicht möglich und ausdrücklich untersagt.

Erfordert ein Use Case einen externen technischen Support, kann sich die Support-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).

VII Rechte der Beschäftigten

1. Datenschutz der Beschäftigten

Die gesetzlichen Anforderungen an die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten sowie gesetzliche Informationspflichten sind zu beachten.

2. Datenverarbeitung

Für die Datenverarbeitung gelten die Datenschutzgrundsätze gem. Art. 5 DS-GVO, die im Intranet einsehbar sind. Auf das Datenverarbeitungsverzeichnis des UK und die Dokumentation im Rahmen des Information Security Management System (ISMS) wird verwiesen.

3. Keine Verhaltens- oder Leistungskontrolle

Anhand der mit den Mobilgeräten erhobenen Daten erfolgt keine Verhaltens- oder Leistungskontrolle der Beschäftigten. Dies gilt nicht für den Fall eines Sicherheits- oder eines Datenschutzvorfalls sowie einer etwaigen Feststellung von Verstößen von Beschäftigten gegen ihre Verpflichtungen aus dieser Dienstvereinbarung, gegen die Nutzungsrichtlinien oder gegen gesetzliche Verpflichtungen, für die das UK sich nach individueller Prüfung arbeits- oder disziplinarrechtliche Maßnahmen vorbehält.

4. Keine personellen Einzelmaßnahmen

Informationen, die das UK unter Verstoß gegen diese Dienstvereinbarung gewinnt, dürfen keine Grundlage für personelle Einzelmaßnahmen gegen Beschäftigte sein.

VIII Übergangsbestimmung

Für Beschäftigte des UK, die bei Abschluss dieser Vereinbarung bereits ein Mobilgerät der Geräteklassifizierung Personal Device (III 3.) nutzen, gilt diese Vereinbarung erst ab dem nächsten Gerätewechsel der Personal Device. Bis dahin gelten für diese Beschäftigte für die Nutzung ihrer Personal Device die bisherigen Regelungen des Zentrums für Informations- und Medizintechnik.

IX Schlussbestimmungen

Sollte eine Bestimmung dieser Dienstvereinbarung unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine dieser Bestimmung möglichst nahekommende wirksame Regelung zu treffen. Sollten die Parteien keine Einigung über die Auslegung dieser Vereinbarung erzielen können, kann jede Seite die ständige Einigungsstelle anrufen.

Diese Dienstvereinbarung tritt am Tage ihrer Unterzeichnung in Kraft. Sie ist mit einer Frist von 24 Monaten zum Ablauf eines Kalenderjahres, erstmals zum 31.12.2022, durch schriftliche Erklärung gegenüber dem Betriebspartner kündbar.

Im Falle einer Kündigung treten die Parteien unmittelbar zu Nachverhandlungen zusammen.

Die Dienststelle gibt diese Dienstvereinbarung ihren Mitarbeitern in geeigneter Weise bekannt.

Für das Universitätsklinikum

Heidelberg, den 17.03.2020

Dipl. [illegible] Hartmut Masanek
Kom[illegible]er Kaufmännischer Direktor
Un[illegible]Heidelberg
Im [illegible] Feld 672
69120 Heidelberg

Für den Personalrat des Universitätsklinikums

Heidelberg, den 18.03.2020

UNIVERSITÄTS
KLINIKUM
HEIDELBERG

ZIM Zentrum für Informations- und Medizintechnik

Mobile Devices - MDM-Systemsteckbrief
Anlage 1 DV Mobile Devices

Im Folgenden sind die Einstellungen des UK Mobile Device Management Systems (MDM System) festgelegt, soweit sie die Themen Beschäftigten-, Persönlichkeits- und Datenschutz (zusammengefasst unter dem Begriff „Privacy“) betreffen. Die Einstellungen dürfen nur in gemeinsamer Abstimmung der Unterzeichner der Dienstvereinbarung zu Mobile Devices geändert werden und gelten einheitlich für das UK.

I Server Systeme

1. MDM-System

Eckdaten der UK MDM-Instanz:

- Produkt und Hersteller — AirWatch - Workspace ONE UEM von VMware
- Standort der MDM-Server/Datenbank — UK eigene Rechenzentren
- Administration MDM-System — durch UK Personal (ZIM)

2. Externe Management Dienste

Entsprechend dem Stand der Technik nutzen die mobilen Geräte für bestimmte Funktionen (z. B. App-Store, Push-Nachrichten, Installation) allgemeine Managementdienste der jeweiligen Hersteller:

- Geräte-/Systemhersteller — Android/Google, iOS/Apple, Samsung
- MDM-Lieferant — VMWare AirWatch

II Hinweise zu Privacy-Einstellungen

Die Angaben beziehen sich nur auf die vom MDM-System zentral erfassten Daten und Einstellungen. Die lokal auf dem Gerät aktivierten Optionen können davon abweichen (z. B. kann ein Anwender GPS lokal auf einem Gerät aktivieren, auch wenn das MDM-System dies nicht zentral ausliest).

Es wird zwischen Shared und Personal Devices unterschieden.

Einstellungsoptionen:

- Optionen bei erfassten Daten
  aktiv - die Daten werden erfasst und auf der MDM-Admin-Konsole angezeigt / *intern* – die erfassten Daten werden nur MDM-programmintern (z. B. um unsichere Apps auszuschließen) verwendet, die konkreten Datenwerte sind für die MDM-/Support-Administration des UK nicht einsehbar / *inaktiv* - die Daten werden nicht gesammelt
- Optionen bei Admin-Befehlen
  möglich - die MDM-/Support-Administration kann den Befehl direkt ausführen / *Rückfrage* - der Anwender muss den Befehl freigeben / *verhindert* - die MDM-/Support-Administration kann den Befehl nicht starten

III MDM Privacy Einstellungen

1. Erfasste Daten

Name der Einstellung	Wert bei Shared D.	Wert bei Personal D.	Zusätzliche Hinweise/Begründung
Geräte Mobilnummer	Aktiv	Aktiv	Benötigt, um zu sehen (z. B. im Rahmen von Fehleranalysen), welche Telefonnummer (=zugeordneter Mobilfunkvertrag) ein Gerät verwendet.
Installierte Profile	Aktiv	Aktiv	Profile geben die Konfiguration eines Gerätes vor. Es ist daher sehr wichtig zu sehen, welche Profile auf einem Gerät vorhanden sind.
Installierte Apps	Aktiv	Intern	Bei Shared Devices muss geprüft werden können, ob exakt die für den Use Case benötigten Apps vorhanden sind. Bei Personal Devices muss die Möglichkeit gegeben sein, Apps z. B. aus Gründen der Informationssicherheit zu verbieten.
Geräte IP-Adresse	Aktiv	Intern	Shared Devices sollen nur über Unternehmensnetzwerke zugreifen. Bei Personal Devices soll der Zugriff über fremde Netze verhindert werden können, wenn Belange der Informationssicherheit, des Datenschutzes oder der betrieblichen Nutzung dem widersprechen.
Telekomanbieter/Länder Code	Aktiv	Intern	Shared Devices sollen i. d. R nur über UK-Mobilfunkanbieter zugreifen. Bei Personal Devices soll Zugriff über fremden Provider bei Bedarf verboten werden können.
GPS Data	Aktiv	Inaktiv	Sporadische Standorterfassung/Historie - kein Live-Tracking, bei Shared: Auffindbarkeit + Geofencing für kritische Use Cases wichtig. Bei Personal Devices kann darauf verzichtet werden.
Telefonie-/Daten/SMS/Roaming-Nutzung	Inaktiv	Inaktiv	Generell keine Auswertung/Regeln hinsichtl. Nutzungsvolumen im MDM. Volumen-/Kostenbetrachtung erfolgt über Rechnung des Mobilfunkanbieters

2. Administrative Befehle

Name der Einstellung	Wert Shared	Wert Personal	Zusätzliche Hinweise/Begründung
Device Löschen	möglich	möglich	Bei Verlust muss vollständiges Löschen durch IT-Admin möglich sein. Hinweis: Bei Personal Dev. erst nach organisatorisch geregelter Frist.
Device sperren/Passcode zurücksetzen	möglich	möglich	Bei Verlust muss Sperre durch Support-Admin möglich sein. Rücksetzen des Passcodes auf Anwenderwunsch durch Support notwendig (analog Windows AD-Passwort)
Datei-/Registry-Zugriff, Remote Control, Request Device Log	Verhindert	Verhindert	Für Betrieb seitens Support-Admin nicht benötigt.

3. Persönliche Datenattribute

Im MDM-System werden folgende persönliche Anwenderattribute verwendet (aus Windows AD-Domäne): Name, Useraccount, E-Mail-Adresse, Telefonnummer

IV MDM Berechtigungsrollen

Im Rahmen der Administration mobiler Endgeräte sind folgende Berechtigungsrollen definiert:

Rollenname/ Org. Gruppe	Aufgabenbeschreibung	Berechtigungen
Support-Administration Zentraler ZIM Mobile Device Support	Verwaltung der im MDM verwalteten Geräte und User im Rahmen des Anwendersupports.	■ Mobile Endgeräte administrieren (z. B. hinzufügen, löschen, sperren) ■ User administrieren (z. B. freischalten, berechtigen) ■ Zuordnung vordefinierter Use Cases, Apps und Zugriffen zu Geräten/Usern ■ Einsehen von Geräte-Betriebs-informationen (z. B. Standort, inst. Apps) soweit dies entsprechend den o. g. Privacy Einstellungen möglich ist
MDM-Administration Zentraler ZIM IT-Systembetrieb	Installation und Konfiguration des MDM	■ Alle Berechtigungen der Rolle „Support-Administration“ (s.o.) ■ Ändern der MDM-Systemeinstellungen (inkl. der o.g. Privacy-Einstellungen) ■ Verwaltung der MDM-Berechtigungsrollen ■ Einpflegen von Use Cases, Apps und mobilen Zugriffen ■ Einsehen der MDM-weiten Protokollierungen und Leistungsdaten
User Nutzer mobiler Endgeräte	Nutzer und Verantwortlichen eines mobilen Endgerätes steht ein Self Service Portal (Web-Anwendung) zur Verfügung.	■ Self-Service Informationen und Aktionen für die eigenen Geräte (z. B. Klingeln lassen, Sperren, Standort) Hinweis: Das Self-Service-Portal ist eine von der Administrationsoberfläche (s. vorherige Rollen) getrennte Anwendung

UNIVERSITÄTS
KLINIKUM
HEIDELBERG

ZIM Zentrum für Informations- und Medizintechnik

Mobile Devices - Antrag Personal Device (Anlage 2 DV Mobile Devices)

I Antragsdaten

Antragssteller (Nutzer)

Nachname _____ Vorname _____

Abteilung _____ Telefon für Rückfragen _____

E-Mail-Adresse _____

Kostenstellenverantwortliche Person

Mandantenkürzel _____ Kostenstellennummer _____

Verantwortl. Nachname _____ Verantwortl. Vorname _____

Gerätedaten

Beantragt. Gerätemodell
(aus UKHD Warenkorb) _____

Antragsart ☐ Neu ☐ Ersatz-Verlust ☐ Ersatz-Defekt ☐ Tausch-Anderes Modell

Nur bei Ersatz/Tausch (Hinweis: das bisherige Gerät ist bei Defekt/Tausch zurückzugeben):

Bisherige Rufnummer _____

Bisheriges Gerätemodell _____ IMEI-Nummer _____

Fehlerbeschreibung _____

II Option zur privaten Nutzung

Bei persönlich zugeordneten Unternehmensgeräten besteht die Möglichkeit, dieses auch für private Zwecke (z. B. Telefonie, Internet) zu verwenden. Der Nutzer kann frei entscheiden, ob er hiervon Gebrauch macht. Die Nutzungsbedingungen hierfür sind:

- Durch die private Nutzung darf die dienstliche Verwendung nicht beeinträchtig werden.
- Die Privatnutzung darf keine Kosten verursachen, die die vereinbarte Nutzungspauschale übersteigen.
- Die aktuellen Tarifbedingungen sind im Intranet veröffentlicht.
- Der Nutzer nimmt in Kauf, dass bei privater Nutzung grundsätzlich ein Risiko besteht, dass es zu unerwünschten Überschneidungen zwischen dienstlichen und privaten Bereichen auf dem Gerät kommen kann.
- Der Nutzer akzeptiert, dass hierfür nur ein eingeschränkter Anwendersupport geliefert wird.
- Für die Nutzung (insb. Hardware, Telefonie, Datenverkehr) erhebt das Unternehmen eine Nutzungspauschale. Kosten für zu rein privaten Zwecken installierten Apps sind hierin nicht enthalten. Private Apps müssen über einen eigenen, privaten Account (Apple-/Google-ID) erworben werden.

  Die Nutzungspauschale beträgt 10,00 € je Monat und wird monatlich vom Netto-Gehalt des Nutzers abgezogen.

Durch Antragssteller (Nutzer) gewählte Option:

☐ Ich werde das Mobilgerät dienstlich nutzen

☐ Ich möchte das Mobilgerät auch privat nutzen und erkläre mich mit den obigen Bedingungen und der von mir persönlich zu begleichenden Nutzungspauschale einverstanden

III Nutzungsrichtlinie zu Mobile Devices

Für die Verwendung von Mobilgeräten gelten am Universitätsklinikum Heidelberg die „Mobile Device Nutzungsrichtlinie“ und die „Dienstvereinbarung Mobile Devices“. Beide Dokumente habe ich zur Kenntnis genommen und werden mir im Intranet zur Verfügung gestellt.

IV Nutzung personenbezogener biometrischer Daten

Das UK überlässt dem Nutzer die Entscheidung, ob er die lokale Biometriefunktion der Geräte (z. B. Fingerabdruck für die Gerätesperre) verwenden möchte. Mit meiner Unterschrift willige ich ein, dass meine persönlichen biometrischen oder daraus abgeleitete Daten lokal auf dem Mobilgerät abgespeichert werden

V Einverständniserklärung und Freigabe

1. Antragssteller (Nutzer)

Ich bestätige die Richtigkeit der Angaben und Einhaltung der o. g. Bedingungen:

Ort, Datum Unterschrift

2. Kostenstellenverantwortliche Person

Ich gebe den Antrag und Abrechnung über die o.g. Kostenstelle frei

Ort, Datum Unterschrift

UNIVERSITÄTS
KLINIKUM
HEIDELBERG

ZIM Zentrum für Informations- und Medizintechnik

Mobile Devices - Nutzungsrichtlinie

Mobile Geräte wie Smartphones und Tablets werden am Universitätsklinikum Heidelberg aufgrund ihrer Flexibilität und Benutzerfreundlichkeit sowohl als Kommunikationsmittel als auch für klinische und betriebliche Fachanwendungen eingesetzt. Neben den Vorteilen dieser Geräte ergeben sich aber auch Gefahren, insbesondere in den Bereichen Persönlichkeits- und Datenschutz sowie der IT-Sicherheit.

Diese Risiken können durch verantwortungsvolles Handeln der einzelnen Anwenderinnen und Anwender minimiert werden. Die folgenden Verhaltensregeln richten sich daher direkt an die Nutzer von unternehmenseigenen Mobilgeräten und sind bindend.

I Das Wichtigste

1. Support

Zentraler Anwendersupport für mobile Endgeräte (Smartphones und Tablets):

- Platzhalter für den jeweils gültigen Intranet-Link
- Zum Zeitpunkt der DV-Freigabe ist dies
  http://intranet.krz.uni-heidelberg.de/index.php?id=5744

Insbesondere bei folgenden Ereignissen müssen Sie sich zeitnah und direkt an den Support wenden:

- Wenn das Mobilgerät verloren wurde oder in die Hände Unbefugter gelangt ist
- Bei Verdacht, dass das Gerät manipuliert wurde (z. B. unbekannte Apps/Netzwerkzugriffe)
- Bei Problemen/Defekten, die sich auf die Patientenversorgung signifikant auswirken

2. Geräteschutz und Gerätesperre

Schützen Sie das Gerät vor Diebstahl und Fremdzugriff insbesondere in öffentlichen Bereichen (z. B. Flure, Patientenzimmer, Außengelände).

Geben Sie das Mobilgerät nicht unbeaufsichtigt an Dritte weiter d.h. weder an unbeteiligte Beschäftigte noch an Externe wie z. B. Geschäftspartner oder Dritte im lebensnahen bzw. persönlichen Umfeld.

Zugangsdaten sind streng vertraulich zu behandeln und dürfen Dritten nicht zugänglich gemacht werden.

Achten Sie darauf, dass die Displaysperre bei Nichtnutzung aktiv ist und dass diese sich zeitgesteuert automatisch einschaltet.

Grundsätzlich sind eine mindestens 4-stellige PIN oder lokale Biometriefunktion des Mobilgerätes (z. B. Fingerabdruck; Nutzung ist freiwillige Entscheidung des Anwenders) als Zugriffsschutz zulässig. Die in einem Nutzungsszenario zulässige Art der Gerätesperre wird durch das UK vorgegeben.

Bei im Team genutzten Geräten ändern Sie die Sperre nicht eigenständig, sondern stimmen Sie sich mit anderen Nutzern im Team ab.

II Nutzung

1. Verantwortungsvoller Umgang

Mobilgeräte und Zubehör sind Eigentum des Klinikums und werden den Beschäftigten zur Nutzung anvertraut. Bitte gehen Sie daher sorgfältig damit um und verwenden Sie die Geräte nur für den vorgesehenen Einsatzzweck.

Shared und Personal Devices:

Grundsätzlich unterscheiden wir zwischen zwei Gerätegruppen

- „Shared Devices“ werden von einem Team gemeinsam genutzt und sind auf einen definierten betrieblichen Einsatzzweck zugeschnitten. Diese Geräte dürfen durch die Nutzer nicht eigenhändig verändert werden.
- „Personal Devices“ sind einer konkreten Person zugeordnet und dienen insbesondere der Kommunikation (Telefonie, E-Mail, Kalender). Der Nutzer kann das Gerät innerhalb der technischen Richtlinien den eigenen Wünschen anpassen, sofern die dienstliche Nutzung hierdurch nicht eingeschränkt wird.

2. Privatnutzung (in Verbindung mit Nutzungspauschale)

Bei Shared Devices ist die Nutzung für private, nicht-dienstliche, Zwecke generell nicht gestattet.

Bei Personal Devices kann sich der Nutzer bei Zuteilung eines Mobilgerätes entscheiden, ob er es - unter Zahlung einer Nutzungspauschale - auch für private Zwecke nutzen möchte. Nähere Informationen zur privaten Nutzung stehen im Antragsformular.

3. Installieren von Apps

Alle dienstlich benötigten Anwendungen werden über den UK App Store bereitgestellt. Sollten Sie eine dienstliche App vermissen, wenden Sie sich bitte an den o.g. Support.

Auf Shared Devices sind bereits alle benötigten Apps vorinstalliert. Es dürfen keine Apps vom Nutzer hinzugefügt oder entfernt werden.

Bei Personal Devices mit privater Nutzung können Sie zusätzliche Apps mit Ihrer privaten Apple-/Google-ID aus dem iOS/Android-App-Store installieren, sofern diese nicht die betriebliche Nutzung beeinträchtigen oder nicht von der MDM-Administration gesperrt wurden.

4. Keine wichtigen Daten lokal speichern

Bei Mobilgeräten ist aufgrund Ihrer Hardware und Bauform grundsätzlich damit zu rechnen, dass sie ausfallen oder abhandenkommen. Sie sind daher kein sicherer Datenspeicher. Es erfolgt kein Backup.

Bei betrieblichen Anwendungen liegen die Daten i. d. R. automatisch auf dem entsprechenden Server. Sollten Sie Daten manuell erzeugt haben, kopieren Sie diese auf Unternehmens-Server bzw. bei privater Nutzung auf entsprechende externe Dienste.

5. WLAN-Zugang

Für Shared Devices ist das WLAN für die Gerätenutzung am Unternehmensstandort betriebsfertig eingerichtet und darf nicht verändert werden. Bei Personal Devices können Sie nach Ihrem Bedarf WLAN-Netze hinzufügen, um z. B. das Gerät zuhause über Ihr Heimnetz zu nutzen.

III Beschäftigten - und Datenschutz

1. Keine Pflicht zur Erreichbarkeit

Die betriebliche Nutzung des Mobilgeräts erfolgt grundsätzlich nur innerhalb der vertraglichen Arbeitszeit der Beschäftigten. Arbeitszeit im Sinne dieser Regelung sind auch Bereitschafts- und Rufbereitschaftszeiten. Das Bereithalten eines Mobilgeräts außerhalb der Arbeitszeit darf vom UK nicht angeordnet werden.

2. Datenschutz

Dem UK sind der Schutz personenbezogener Daten und Vertraulichkeit sehr wichtig. Seitens des Unternehmens erfolgt generell keinerlei Zugriff auf die mit den Geräten geführte Kommunikation (Telefonate, E-Mails etc.) oder irgendwelche Auswertungen zum Zweck einer Verhaltenskontrolle.

Soweit möglich sind die Geräte unter Berücksichtigung gesetzlicher Vorgaben im Sinne der Datensparsamkeit so konfiguriert, dass nur so viele personenbezogene Daten gesammelt und zeitlich aufbewahrt werden, wie für den jeweiligen Anwendungsfall unbedingt notwendig.

Um die Einhaltung dieser Grundsätze sicherzustellen und Transparenz herzustellen, werden bei Einführung eines neuen mobilen Nutzungsszenarios die erfassten Daten und Einstellungen dokumentiert und mit den Mitarbeitervertretungen und Datenschutzbeauftragten abgestimmt.

3. Dienstvereinbarung zu Mobile Devices

Um die Interessen der Beschäftigten beim Einsatz von Mobilgeräten zu wahren, sind die Leitlinien in einer Dienstvereinbarung (Dienstvereinbarung Mobile Devices) festgehalten, an der der Datenschutz und die IT-Sicherheit des UK mitgewirkt haben.

IV Mobile Device Administration

1. Mobile Device Management System

Die unternehmenseigenen Geräte und mobilen Zugriffswege werden durch das Mobile Device Management System (MDM) zentral und einheitlich verwaltet.

Zur Sicherstellung der Funktionsfähigkeit, der IT-Sicherheit und des Datenschutzes werden Einstellungen und Richtlinien auf den Mobilgeräten vorgegeben. Versuchen Sie nicht, diese zu umgehen, sondern wenden Sie sich bei Fragen an den o.g. Support.

2. Sperren von Mobilgeräten und Datenlöschung

Bei begründetem Verdacht, dass ein Gerät verloren wurde, in unbefugten Zugriff gelangt oder unsicher ist, kann der Mobile Device Support ein Mobilgerät kurzfristig nach eigenem Ermessen sperren und nach Rücksprache dessen Daten löschen. Einzelheiten zum Verfahren, sind für diese Fälle in der Dienstvereinbarung Mobile Devices geregelt.

Wichtig: Setzen Sie kein Gerät eigenhändig zurück (Werkseinstellungen), sondern wenden Sie sich an den o.g. Support, wenn Sie z. B. eine Neuinstallation wünschen.