Kepler
Universitäts
Klinikum

Geschäftsführung

GZ 405200-2018
5.6.2018

BETRIEBSVEREINBARUNG
über die Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten sowie über den Einsatz von Systemen der Informations- und Kommunikationstechnik

abgeschlossen zwischen der Kepler Universitätsklinikum GmbH, Krankenhausstraße 7a, 4020 Linz, einerseits und dem Zentralbetriebsrat der Kepler Universitätsklinikums GmbH, Krankenhausstraße 9, 4021 Linz, andererseits.

Präambel

Diese Betriebsvereinbarung ersetzt sämtliche geltende Betriebsvereinbarungen, Richtlinien und Regulative der Stadt Linz (bzw. des ehemaligen AKh Linz) sowie der gespag an allen Standorten des Kepler Universitätsklinikums zu den Themen personenbezogene Daten sowie über den Einsatz von Systemen der Informations- und Kommunikationstechnik.

Ziel dieser Betriebsvereinbarung ist es, die Persönlichkeitsrechte der Mitarbeiter/-innen unter Beachtung aller maßgeblichen gesetzlichen Bestimmungen zu sichern und dennoch den Einsatz weitreichender technischer Möglichkeiten sicherzustellen.

Die Unterzeichner dieser Regelung weisen darauf hin, dass Daten über Mitarbeiter/-innen durch die beteiligten Organisationseinheiten nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden (§ 6 Abs. 1 Z 1 DSG 2000).

Die folgenden Regelungen präzisieren diesen gesetzlich angeordneten Grundsatz des Vertrauensschutzes und der Rechtmäßigkeit.

I. Kapitel
Allgemeine Regelungen

§ 1 Geltungsbereich

1. Sachlicher Geltungsbereich

Diese Betriebsvereinbarung gilt für die Verarbeitung von personenbezogenen und/oder personenbeziehbaren Daten unabhängig davon, in welchen Systemen diese Daten gespeichert sind und ob die Verarbeitung in standardisierter oder individueller Form erfolgt.

Diese Betriebsvereinbarung regelt zudem die Einführung, Verwendung und Dateneinsicht bei Systemen und Anlagen zur automationsunterstützten Verarbeitung von Daten (§§ 96 und 96a ArbVG).

2. Persönlicher Geltungsbereich

Die folgenden Regelungen gelten für sämtliche in der Kepler Universitätsklinikum GmbH (im Folgenden „KUK") beschäftigten Mitarbeiter/-innen.

§ 2 Grundsätze der Verarbeitung personenbezogener Daten

In der KUK werden verschiedene automationsunterstützte Systeme eingesetzt, die personenbezogene Daten verwenden. Zum einen sind das Systeme der Personalwirtschaft im engeren Sinne, zum anderen aber auch personalwirtschaftsfremde Systeme. Diese automationsunterstützten Systeme werden zur effizienten Abwicklung der betrieblichen Abläufe eingesetzt.

Bei der Verarbeitung von personenbezogenen Daten sind das Persönlichkeitsrecht des/der Mitarbeiter/-in und das Recht auf informationelle Selbstbestimmung zu beachten. Das bedeutet, dass nicht tiefer in die Persönlichkeitssphäre der Mitarbeiter/-innen eingedrungen werden darf, als es im Rahmen der Zweckbestimmung des Arbeitsverhältnisses erforderlich ist. Darüber hinaus ist das berechtigte Interesse der KUK zu berücksichtigen, wonach die Personaldatenverarbeitung in wirtschaftlich sinnvoller Weise im Rahmen der technischen Möglichkeiten durchgeführt wird.

Das Erheben, Verarbeiten und Auswerten (Nutzen) personenbezogener Daten durch personaldatenverarbeitende Systeme erfolgen nur, soweit dies zur Begründung, Durchführung, Abwicklung und Dokumentation von Arbeitsverhältnissen sowie zur Erfüllung von durch

Rechtsvorschriften begründeten Verpflichtungen oder zum Erstellen von eindeutig anonymisierten Auswertungen erforderlich ist.

Der Zugriff auf die personenbezogenen Daten in den automationsunterstützten Systemen ist auf jene Mitarbeiter/-innen beschränkt, welche diese Informationen zur Erfüllung ihrer betrieblichen Aufgaben benötigen. Dem Zentralbetriebsrat und den Betriebsräten der jeweiligen Standorte ist ab der Unterzeichnung dieser Betriebsvereinbarung halbjährlich eine Liste dieser berechtigten Mitarbeiter/-innen zu übermitteln.

§ 3 Information der einzelnen Mitarbeiter/-innen

Jede/r Mitarbeiter/-in hat das Recht, Auskunft über alle ihn/sie betreffende personenbezogene Daten, welche zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh ohne Automationsunterstützung geführten Dateien bestimmt sind, zu erhalten.

Jede/r Mitarbeiter/-in hat das Recht, Daten richtig stellen oder löschen zu lassen, wenn sie nicht berechtigt ermittelt wurden oder wenn sie nicht richtig sind. Weiters hat jede/r Mitarbeiter/-in das Recht, nach Beendigung des Dienstverhältnisses die Löschung all seiner/ ihrer Daten, für die keine gesetzliche Aufbewahrungspflicht besteht, zu verlangen.

Gegen die Bestimmungen dieser Betriebsvereinbarung erlangte Daten dürfen von der KUK nicht gegen Mitarbeiter/-innen verwendet werden.

§ 4 Übermittlung an Dritte

Übermittlung von personenbezogenen Daten außerhalb des Unternehmens findet nur statt, wenn dazu eine gesetzliche Verpflichtung vorliegt oder dies ausdrücklich in dieser Betriebsvereinbarung vereinbart wurde.

Sämtliche Übermittlungen nach SA015 der Anlage 1 der Standard- Muster-Verordnung 2004 zum Datenschutzgesetz 2000, BGBl. II Nr. 312/2004 i.d.j.g.F. (= Personalverwaltung der Länder, Gemeinden und Gemeindeverbände) sind ohne Befassung des/der Mitarbeiter/-in oder des Betriebsrates des jeweiligen Standortes zulässig.

§ 5 Verwahrung von Geschäftsstücken

Sofern nicht eine strengere Regelung gilt (zB über streng verrechenbare Drucksorten und Gegenstände, vertrauliche Geschäftsstücke, Verschlusssachen), sind Geschäftsstücke nach

Möglichkeit so zu verwahren, dass sie zwar anderen berechtigten Mitarbeiter/-innen auch in Abwesenheit des Verwahrers zugänglich sind, Unbefugten jedoch ein Zugriff verwehrt ist.

Unter Geschäftsstücke sind all jene Unterlagen zu verstehen, die im Zusammenhang mit der dienstlichen Tätigkeit stehen.

§ 6 Allgemeine Regeln für den Zugriff auf Daten und Programme

1. Verwendung von Protokolls- und Dokumentationsdaten

Gemäß § 14 DSG ist Protokoll zu führen, um tatsächliche durchgeführte Verwendungsvorgänge wie insbesondere Änderungen, Abfragen und Übermittlungen im Hinblick auf ihre Zulässigkeit nachvollziehen und kontrollieren zu können.

Zulässig ist die Verwendung der Protokolls- und Dokumentationsdaten aus folgenden Gründen:

- zur Kontrolle der Zulässigkeit der Verwendung des protokollierten und dokumentierten Datenbestandes (Prüfung der Zugriffsberechtigung) sowie
- zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt.

Unzulässig ist die Verwendung der Protokolls- und Dokumentationsdaten:

- zum Zwecke der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind sowie
- zum Zweck der Kontrolle jener Mitarbeiter/-innen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung.

2. Einsichtnahme in Daten und Programme

Die zuständigen Dienstgebervertreter/-innen (Geschäftsführung, Mitglieder der Kollegialen Führung, Geschäftsbereich Personal und Organisation, Vorgesetzte/r) haben bei Bestehen eines begründeten Verdachts einer nicht ordnungsgemäßen Anwendung oder einer strafbaren Handlung (zB Behebung von Fehlfunktionen, Anwendungsproblemen, Nichteinhaltung von Vorgaben und Standards, missbräuchlicher Verwendung von Anwendungsprogrammen, usw) auch ohne Zustimmung des/der Mitarbeiter/-in das Recht, Einsicht in die von ihm/ihr dienstlich verwendeten bzw. nicht verwendeten Daten und Programme zu nehmen. Ob ein begründeter Verdacht vorliegt, entscheiden die zuständigen Dienstgebervertreter/-innen im Einvernehmen mit dem Betriebsrat der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes. Verweigert der Betriebsrat ohne jegliche

Begründung das Einvernehmen, so kann auch ohne seine Zustimmung in die Daten eingesehen werden. In diesem Fall muss der/die betroffene Mitarbeiter/in unter Angabe von Ausmaß und Gründen über die Einsichtnahme informiert werden. Diese Einsichtnahme darf nicht in übersteigender Intensität organisiert sein und jenes Maß überschreiten, das für das jeweilige Arbeitsverhältnis typisch und geboten ist. Der/die Betriebsratsvorsitzende oder eine von ihm/ihr namhaft gemachten Person der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes haben das Recht, bei einer Überprüfung anwesend zu sein.

Bestätigt sich bei einer ersten Einsichtnahme der begründete Verdacht gegenüber einem/einer Mitarbeiter/-in, erhält dieser/diese die Möglichkeit, sich zum Verdacht zu äußern. Er/sie hat das Recht, jederzeit ein Mitglied des Betriebsrates des jeweiligen Standortes beizuziehen. Sollte dem/der Mitarbeiter/-in dieses Recht verwehrt werden, dürfen die erlangten Daten nicht zum Nachteil des Mitarbeiters/der Mitarbeiterin verwendet werden.

Die Einsichtnahme ist entsprechend zu protokollieren (Datum, Name oder User-ID des/der Mitarbeiter/-in, Begründung der Einsichtnahme). Dem/der Mitarbeiter/-in ist eine Ausfertigung des Protokolls zu übergeben. Der/die Mitarbeiter/-in hat das Recht, ihn betreffende Kontrollergebnisse richtigstellen oder löschen zu lassen, wenn sie nicht richtig sind.
Freigestellte Betriebsräte/-innen unterliegen nicht der Kontrolle durch Einsicht in Programme und Daten. Sonstige Mitglieder des Betriebsrates unterliegen jedoch einer solchen Überprüfung, soweit sie nicht im Sinne der Arbeitsverfassung für den Betriebsrat tätig sind. Es gilt die Regelung des § 6 Pkt. 2 dieser Betriebsvereinbarung.

3. Einsatz von Werkzeugen für die Anwenderbetreuung

Die Verwendung von Werkzeugen für die Anwenderbetreuung, die die Spiegelung des Bildschirminhaltes von EDV-Arbeitsplätzen zum/zu jeweiligen Betreuer/-in (das sind zB Mitarbeiter/-innen der IT und deren Dienstleister) ermöglichen, ist unter der Bedingung zulässig, dass dieser Einsatz nur nach vorangegangener Zustimmung seitens des/der jeweiligen Anwenders/-in erfolgt. Unmittelbar vor dem externen Einstieg zur Spiegelung des Bildschirminhalts ist der/die Mitarbeiterin nochmals zu kontaktieren und über den bevorstehenden Vorgang zu informieren.

4. Verbot der Verwendung nicht lizenzierter Software

Auf EDV-Geräten der KUK dürfen nur Programme verwendet werden, an denen die KUK ein Nutzungsrecht hat.

Der Einsatz von sogenannten „Raubkopien" von Computerprogrammen ist auf dienstlichen Computern und auch auf allenfalls für dienstliche Zwecke verwendeten privaten Computern untersagt.

Urheberrechtsverletzungen können für die Geschäftsführung, aber auch für einzelne Mitarbeiter/-innen zivil- und strafrechtliche Konsequenzen haben.

Über Auftrag der Geschäftsführung kann die IT stichprobenartig überprüfen, ob in den Organisationseinheiten nicht lizenzierte Software eingesetzt wird. Der Betriebsrat des jeweiligen Standortes hat das Recht, in die Ergebnisse solcher stichprobenartigen Prüfungen Einsicht zu nehmen. Die Betriebsratsvorsitzenden des jeweiligen Standortes sind unmittelbar nach einer durchgeführten stichprobenartigen Prüfung zu informieren. Bei begründetem Verdacht einer nicht ordnungsgemäßen Anwendung oder einer strafbaren Handlung gegenüber einem/einer Mitarbeiter/-in erfolgt die Vorgangsweise analog zu § 6 Pkt. 2 dieser Vereinbarung.

§ 7 Verbot der privaten Verwendung zu Erwerbszwecken

Die Nutzung dienstgebereigener Anlagen, Programme und Daten zu privaten Erwerbszwecken ist unzulässig, es sei denn, es liegt eine Ausnahmegenehmigung der Geschäftsführung vor.

§ 8 Private Verwendung der IT-Infrastruktur und private Internet-Nutzung

Die private Nutzung der von der KUK zur Verfügung gestellten EDV-Infrastruktur während der Dienstzeit ist nur in begrenztem Maß (nur etwa 15 Minuten pro Tag bzw. etwa 60 Minuten im Nachtdienst, wenn der Dienstbetrieb es zulässt) erlaubt. Unter privater Nutzung ist vor allem das Surfen im Internet, die Bearbeitung privater E-Mails oder das Verfassen privater Schriftstücke zu verstehen.

Eine längere private Internet-Nutzung darf auf Arbeitsplätzen, die der Gleitzeit unterliegen, erst nach dem Ausbuchen am Terminal oder im ESS erfolgen bzw. darf auf Arbeitsplätzen, die keiner Gleitzeit unterliegen, erst nach Ende der Normalarbeitszeit und nach Beendigung zeitlicher Mehrleistungen erfolgen.

Die gelegentliche Nutzung der Informations- und Kommunikationstechnologie des Landes OÖ und der Stadt Linz für private Zwecke außerhalb der Dienstzeit ist gestattet.

Auch im Rahmen der erlaubten Verwendung von dienstlichen Geräten für die private Internet-Nutzung außerhalb der Dienstzeit ist das Betrachten von strafgesetzwidrigen Inhalten

(Pornographie, politischer Extremismus, Gewalt, usw) jedenfalls verboten und unterliegt den gleichen Kontrollmechanismen wie die Internet-Nutzung während der Dienstzeit.

Die private Nutzung darf zudem nicht (weder innerhalb noch außerhalb der Dienstzeit)

- den guten Sitten widersprechen (zB Pornografische Darstellungen),
- einen strafrechtlichen Tatbestand bzw. eine Verwaltungsübertretung auslösen oder unterstützen,
- für eine Nebenbeschäftigung erfolgen (es sein denn, es liegt eine Ausnahmegenehmigung der Geschäftsführung vor),
- Kosten für die KUK verursachen,
- dem Ansehen der KUK abträglich sein,
- wesentliche Interessen derselben verletzen oder
- den einschlägigen Richtlinien der KUK zum Thema IT und Internet-Nutzung widersprechen.

Für die Sicherung und den Schutz privater Daten ist der/die Mitarbeiter/-in selbst verantwortlich.

Der Zugang zu bestimmten Internetseiten kann blockiert werden. Der Zugang zu blockierten Seiten kann jedoch auf bestimmten IT-Arbeitsplätzen freigegeben werden, soweit dies aus dienstlichen Gründen notwendig ist. Als wesentlicher Informationskanal zu den Mitarbeiter/-innen der KUK wird die Verwendung von sozialen Netzwerken durch die Mitarbeiter/-innen der Unternehmenskommunikation sowie durch die Mitglieder und Mitarbeiter/-innen der Betriebsräte an den Standorten und des Zentralbetriebsrates als dienstliche Notwendigkeit bejaht.

§ 9 Vorgangsweise bei eventuellem Änderungsbedarf der Regelungen

Wird erkennbar, dass auf Grund der technisch-organisatorischen Weiterentwicklung Änderungen der gegenständlichen Regelungen erforderlich werden könnten, so hat die Geschäftsführung aufgrund einer Information der zuständigen Organisationseinheit den/die Zentralbetriebsratsvorsitzende/n darüber umgehend zu informieren. Die weitere Vorgehensweise ist daraufhin mit dem Zentralbetriebsrat zu vereinbaren.

§ 10 Mitwirkung des Zentral-/Betriebsrates

Der/Die Zentralbetriebsratsvorsitzende Betriebsratsvorsitzende der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes wird darüber schriftlich informiert, welche Arten von personenbezogenen Daten automationsunterstützt aufgezeichnet werden und welche Verarbeitungen und Übermittlungen vorgesehen sind. Änderungen und Erweiterungen der personenbezogenen Daten werden rechtzeitig vor Einsatz mitgeteilt.

Dem/Der Zentralbetriebsratsvorsitzende/-n und den Betriebsratsvorsitzende/n der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes oder einem von ihm/ihr bestimmten Mitglied des Zentral-/Betriebsrates ist in alle Listen, Auswertungen und Protokolle, die aus den beschriebenen Systemen gewonnen werden, nach Maßgabe der Bestimmungen des ArbVG Einsicht zu gewähren. Insbesondere kann er/sie auch in jene Bereiche des Systems Einsicht nehmen, in denen diese Listen verwaltet werden.

Eine Übersicht aller Systeme, die personenbezogene Daten verarbeiten, unter Angabe der von ihnen erfassten Daten und der Art der Datenverarbeitung findet sich im Datenverarbeitungsregister. Den Zentral-/Betriebsratsvorsitzenden ist auf Verlangen Einsicht in dieses Register zu gewähren.

Einsicht in konkrete Daten einzelner Mitarbeiter/-innen haben der/die Zentralbetriebsratsvorsitzende und die Betriebsratsvorsitzenden der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes bzw. die von ihnen bestimmten Zentral-/Betriebsratsmitglieder nur, wenn dies durch gesetzliche Bestimmungen oder diese Betriebsvereinbarung erlaubt wird oder der/die betroffene Mitarbeiter/-in zustimmt. Eine Einsicht in den Personalakt von Mitarbeitern/-innen ist nur mit deren Zustimmung möglich.

II. Kapitel
Spezielle Regelungen bzgl. Auswertungen

§ 11 Zeiterfassung/elektronischer Dienstplan

1. Abfragen von Zeitdaten

Das Abfragen von Zeitdaten, welche den Zeitraum von zwei Jahren vor Datum der Abfrage betreffen, ist ohne Zustimmung der Mitarbeiter/-innen durch den/die Vorgesetzte/n, durch die Mitarbeiter/-innen des Geschäftsbereichs Personal und Organisation und durch die/den Zeitbeauftragte/n zulässig.

Bei Abfragen, welche über einen Zeitraum von zwei Jahren ab Datum der Abfrage hinausgehen, bedarf es einer vorhergehenden schriftlichen Information des/der Mitarbeiter/-in über das Ausmaß und die Gründe der Abfrage.
Sollte nach einer Abfrage der Zeitdaten ein begründeter Verdacht auf eine Dienstpflichtverletzung vorliegen, so wird analog die Regelung des § 6 Pkt. 2 angewendet.

Nach Ende jeden Kalendermonats ist dem/der Mitarbeiter/-in vom dem/der Zeitbeauftragten eine Dienstzeitaufzeichnung (Monatsjournal) auszuhändigen, sofern für den/die Mitarbeiterin keine andere Informationsmöglichkeit über seine/ihre Zeitaufzeichnungen besteht.

2. Korrektur von Zeitdaten

Die Zeiterfassungsdaten werden zentral gespeichert. Korrekturen werden elektronisch protokolliert.

Die Korrektur von Zeitdaten bei offensichtlichen Fehlbuchungen (zB Doppelbuchungen oder Buchungen im Urlaub/ Krankenstand), die das laufende und vorangegangene Monat betreffen, ist ohne Zustimmung des/der Mitarbeiters/-in durch den/die Vorgesetzte, durch die Mitarbeiter/-innen des Geschäftsbereichs Personal und Organisation und durch den/die Zeitbeauftragte/n zulässig. Der/die Mitarbeiter/-in ist unmittelbar über das Ausmaß und die Gründe der Korrektur zu informieren

Die Korrektur von Zeitdaten, die über das laufende und vorangegangene Monat hinausgehen, ist ohne Zustimmung des/der Mitarbeiters/-in nur zulässig, wenn der/die Mitarbeiter/-in und der Betriebsrat der zu vertretenden Arbeitnehmer/-innengruppe des jeweiligen Standortes zuvor schriftlich über das Ausmaß und die Gründe der Korrektur informiert wird.

Bei Korrekturen von Zeitdaten, welche über einen Zeitraum von einem Jahr ab Datum der Abfrage hinausgehen, ist zusätzlich der/die Betriebsratsvorsitzende der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes zu informieren.

§ 12 Leistungserfassung (zB für Mitarbeiter/-innen der IT und der technischen Betriebsdienste oder in klinischen Systemen)

1. Allgemeines

Die Daten der einzelnen Organisationseinheit sind so abgeschottet, dass nur berechtigte Mitarbeiter/-innen Zugriff auf die Daten haben. Der/die für die Leistungserfassung beauftragte Mitarbeiter/-in muss die Möglichkeit haben, manuelle Eingaben zu machen.

2. Abfragen von Leistungserfassungsdaten

Der/die Mitarbeiter/-in kann zeitlich unbeschränkt seine eigenen Leistungserfassungsdaten abfragen (solange die Daten im direkten Zugriff der Datenbank liegen).

Berechtigte Mitarbeiter/-innen im Bereich Rechnungswesen, im Geschäftsbereich Personal und Organisation und der/die Vorgesetzte können für das laufende oder vorangegangene Kalenderjahr Leistungserfassungsbelege abfragen. Bei Abfragen, welche über einen Zeitraum von einem Jahr ab

Datum der Abfrage hinausgehen, bedarf es einer vorhergehenden Information des/der Mitarbeiter/-in oder des/der Betriebsratsvorsitzenden der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes.

3. Korrektur von Leistungserfassungsdaten

Der/die Mitarbeiter/-in kann für das laufende und die zwei vorangegangenen Kalendermonate Korrekturen der Leistungserfassungsdaten vornehmen, wobei ausschließlich Ergänzungen möglich sind.

Berechtigte Mitarbeiter/-innen im Bereich Rechnungswesen, im Geschäftsbereich Personal und Organisation und der/die Vorgesetzte können für das laufende und vorangegangene Kalendermonat ohne Zustimmung des/der Mitarbeiter/-in Korrekturen bei offensichtlicher Fehlerfassung vornehmen.

Die Korrektur von Leistungsdaten, die über das laufende und vorangegangene Monat hinausgehen, ist ohne Zustimmung des/der Mitarbeiters/-in nur zulässig, wenn der/die Mitarbeiter/-in zuvor über das Ausmaß und die Gründe der Korrektur informiert wird.

Bei Korrekturen von Leistungsdaten, welche über einen Zeitraum von einem Jahr ab Datum der Abfrage hinausgehen, ist zusätzlich der/die Betriebsratsvorsitzende der zu vertretenden Arbeitnehmergruppe des jeweiligen Standortes zu informieren.

§ 13 Dokumentation in betriebswirtschaftlichen und medizinischen Systemen (wie zB SAP, ...)

Alle Prozessschritte in der Dokumentation sind in mehreren Protokolltabellen technisch in einer Datenbank abgelegt. Die Auswertung dieser technischen Protokolle ist nur mit speziellen Berechtigungen möglich.

Diese technische Berechtigung wird benötigt, um Programm-, Ablauf- und Bedienungsfelder evaluieren zu können. Es werden auch verschiedene Möglichkeiten für Auswertungen pro UserID angeboten, zB durchschnittliche Liegezeit, durchschnittliche Bearbeitungsdauer, usw. Diese speziellen Berechtigungen haben nur die Betreuer der IT.

Innerhalb der Organisationseinheit ist den Vorgesetzten zur Wahrnehmung der unmittelbaren Führungsverantwortung und zur gezielten Steuerung des Personal- und Ressourceneinsatzes sowie für Benchmarking-Zwecke eine Auswertung möglich.

Bei Vorliegen eines begründeten Verdachtes auf nicht ordnungsgemäße Anwendung (zB Behebung von Fehlfunktionen, Anwendungsproblemen, Nichteinhaltung von Vorgaben und Standards, Probleme bei der Auslastung, ...) ist eine personenbezogene Auswertung der technischen Protokolle nur unter Beachtung der unter § 6 Pkt. 2 definierten Vorgangsweise zulässig.

Insbesondere ist bei begründetem Verdacht unter Beachtung der unter § 6 Pkt. 2 definierten Vorgehensweise auch ein Vergleich der Dienstplan-Daten mit jener der Garagenbenützungs-Daten möglich, um An- und Abwesenheiten kontrollieren zu können.

§ 14 Internet und E-Mail-Nutzung

1. Internet-Nutzung

Der Dienstgeber kann zur grundsätzlichen Erhebung des Internetverhaltens von Mitarbeiter/-innen bei der IT eine anonymisierte Auswertung darüber in Auftrag geben, welche Internet-Server und Seiten von der Gesamtheit der Mitarbeiter/-innen oder einer Organisationseinheit (Mindestgröße fünf Mitarbeiter/-innen) am häufigsten angewählt wurden.

Bei begründetem Verdacht des Missbrauchs (zB Kapazitätsprobleme, Nutzung zu privaten Erwerbszwecken, Nutzung, die den Interessen und dem Ansehen der KUK in der Öffentlichkeit schaden kann, die gegen gesetzliche Bestimmungen verstößt, private Nutzung innerhalb der Dienstzeit in nicht unwesentlichem Ausmaß, Chatten, Glückspiel, usw) kann der Dienstgeber Internetaktivitäten prüfen, die sich auf einen konkreten EDV-Arbeitsplatz oder User beziehen. Diese Überprüfung hat unter Beachtung der unter § 6 Pkt. 2 definierten Vorgangsweise zu erfolgen.

Soll überprüft werden, ob die Internet-Nutzung tatsächlich in Erfüllung dienstlicher Aufgaben erfolgt ist, ist eine solche Überprüfung ohne Zustimmung des/der Mitarbeiter/-in nur dann zulässig, wenn ein begründeter Verdacht auf eine Dienstpflichtverletzung und/oder strafbare Handlung vorliegt. Es ist die unter § 6 Pkt. 2 definierten Vorgangsweise einzuhalten.

Freigestellte Betriebsräte/-innen unterliegen bezüglich der Nutzung von Internet und E-Mail keiner Überprüfung ihres individuellen Nutzungsverhaltens. Sonstige Mitglieder des Zentral/-Betriebsrates unterliegen jedoch einer solchen Überprüfung, soweit sie nicht im Sinne der Arbeitsverfassung für den Zentral-/Betriebsrat tätig sind. Es ist die unter § 6 Pkt. 2 definierte Vorgangsweise einzuhalten.

2. E-Mail-Nutzung

E-Mails unterliegen dem Briefgeheimnis (§ 118 StGB).

Soll überprüft werden, ob E-Mails tatsächlich in Erfüllung dienstlicher Aufgaben getätigt wurden, ist eine solche Überprüfung ohne Zustimmung des/der Mitarbeiter/-in nur dann zulässig, wenn ein begründeter Verdacht auf eine Dienstpflichtverletzung und/oder strafbare Handlung vorliegt. Es ist die unter § 6 Pkt. 2 definierte Vorgangsweise einzuhalten.

§ 15 Kontrolle von Telefondaten

Die in der Telefondatenbank bezüglich der Höhe der Gesprächskosten gespeicherten Daten über dienstliche und private Gespräche im Festnetz können vom Dienstgeber nach Organisationseinheiten (Mindestgröße fünf Mitarbeiter/-innen) geordnet kontrolliert werden.

Für Mobiltelefone, Einzelanschlüsse in Außenstellen und Kleinanlagen mit weniger als fünf Nebenstellenanschlüssen, für die eine Anonymisierung der Gesprächskosten aus technischen bzw. organisatorischen Gründen nicht möglich ist, dürfen bei begründetem Verdacht einer Dienstpflichtverletzung auch einzelne Nebenstellen, Einzelanschlüsse bzw. Mobiltelefone einer Kontrolle unterzogen werden. Es ist die unter § 6 Pkt. 2 definierten Vorgangsweise einzuhalten.

Wird überprüft, ob die als dienstlich gekennzeichneten Gespräche (Telefonnummern) tatsächlich in Erfüllung dienstlicher Aufgaben getätigt wurden, ist die unter § 6 Pkt. 2 definierten Vorgangsweise einzuhalten.

Das Ab- und Mithören von Telefongesprächen seitens des Dienstgebers ist unzulässig.

§ 16 Betriebsdatenerfassung

Im Rahmen der Betriebsdatenerfassung werden unter anderem Daten über

- den berechtigten Zutritt zu Gebäuden, Gebäudeteilen und Parkplätzen,
- konsumierte Speisen und Getränke und
- Versorgung mit Berufskleidung, usw.

erfasst.

Personenbezogene Auswertungen sind nur auf Antrag des/der Mitarbeiters-/in,zum Zwecke der Behebung von Fehlbuchungen, der Verrechnung, der Kostenrechnung und des Nachweises eines berechtigten Zutritts zulässig.

Darüber hinaus sind personenbezogenen Einsichtnahmen in die protokollierten Daten ohne Zustimmung des/der Mitarbeiter/-in nur zulässig, wenn ein begründeter Verdacht auf eine

Dienstpflichtverletzung und/oder strafbare Handlung vorliegt. Es ist die unter § 6 Pkt. 2 definierten Vorgangsweise einzuhalten.

1. Elektronisches Zutrittssystem

Das elektronische Zutrittssystem ermöglicht außerhalb der Öffnungszeiten den Zutritt zu Gebäuden der KUK.

Die Zugangstüren der Gebäude und Räume der KUK können mit einem elektronischen Zutrittssystem ausgestattet werden.
Die KUK hat das Recht, das verwendete System stets am aktuellen Stand der Technik zu halten. Kommt es zu einer Erweiterung bzw. grundlegenden Funktionsänderung des Systems, sind der/die Betriebsratsvorsitzende des jeweiligen Standortes, der/die Zentralbetriebsratsvorsitzende und die/der Datenschutzbeauftragte davon zu informieren.

2. RF-ID Chips bzw. RF-Laundry Chips

Für die Zuordnung von Kleidungsstücken zu den Bediensteten (individuellen Träger/-innen) bzw. zum jeweiligen Standort befinden sich in der Dienstkleidung, welche zum Teil von der KUK selbst und zum Teil von der Vertragsfirma zur Verfügung gestellt wird, RF-ID Chips bzw. RF-Laundry Chips.

Auf den RF-ID Chips werden allgemeine Daten (Eigentümer des Wäschestückes, Kleidergröße, Anzahl der Waschzyklen, Standort allgemein) und auf den RF-Laundry Chips neben allgemeinen Daten auch personenbezogene Daten (Name des/der Trägers/-in und Organisationseinheit bzw. Standort) gespeichert. Die gespeicherten Daten dienen lediglich der Zuordnung im Logistik-Prozess.

Der Einsatz von aktiven RF-ID Chips findet nicht statt.

§ 17 E-Learning Programme

Sofern Mitarbeiter/innen gesetzlich vorgesehene Schulungen absolvieren müssen, kann dies auch in Form von E-Learning-Programmen erfolgen. Werden durch die Absolvierung dieser Programmen personenbezogene Daten verarbeitet, so ist dies nur durch den Zweck der rechtlichen Verpflichtung für diese Schulung gedeckt (zB Datenschutzschulung, Brandschutzschulung, usw).

§ 18 Wartung und Fehlerbehebung

Im Rahmen von Fehleranalysen sind Datenerhebungen zulässig. Die erhobenen Daten dürfen nur zur Analyse und zur Behebung eines technischen Problems dienen und sind unverzüglich zu löschen.

§ 19 Schlussbestimmungen

1. Inkrafttreten

Die gegenständliche Vereinbarung tritt mit dem auf den Tag der Kundmachung folgenden Tag in Kraft.

2. Geltungsdauer

Die Betriebsvereinbarung wird unbefristet abgeschlossen und kann von beiden Vertragspartnern unter Einhaltung einer 3-monatigen Kündigungsfrist jeweils zum Quartalsende gekündigt werden

Für die Kepler Universitätsklinikum GmbH:

Linz, am 26.6.2018

Mag.[a] Dr.[in] Elgin DRDA	Dr. Heinz BROCK, MBA, MPH, MAS	Simone POLLHAMMER, MBA
Kaufmännische Direktorin	Ärztlicher Direktor	Pflegedirektorin
Geschäftsführerin	Geschäftsführer	

Für den Zentralbetriebsrat der Kepler Universitätsklinikum GmbH:

Linz, am .....

Branko NOVAKOVIC
Vorsitzender des Zentralbetriebsrates