KlinikService
Gesellschaft am Universitätsklinikum Heidelberg mbH

Anlage 5.3
Datenschutz/Zweckbestimmung

Die Verarbeitung personenbezogener Daten richtet sich nach den Grundsätzen der Zweckbindung, Normenklarheit und Verhältnismäßigkeit ANL 3.1:

Zweckbindungsgrundsatz bei der Verarbeitung personenbezogener Daten

Der Umgang mit personenbezogenen Daten durch den Arbeitgeber erfolgt für konkret festgelegte, eindeutige und legitime Zwecke unter der Beachtung der Grundsätze des Art. 5 Abs. 1b DSGVO und insbesondere der in Art. 88 Abs. 1 DSGVO benannten Zwecke und der in § 26 Abs. 1 S. 1,2 BDSG bezeichneten Zwecke.

Personenbezogene Daten der Beschäftigten im Rahmen dieser Betriebsvereinbarung dürfen nicht mit anderen internen Dateien oder EDV-Systemen verknüpft werden.

Ausnahmen bestehen in den folgenden Punkten, sofern dies im Rahmen des in § 3 genannten Zwecks geschieht:

- Verknüpfung mit der Weitergabe von Daten an das Rechnungswesen

- Überprüfung des aktuellen Standes der Soft- und Hardware-Konfiguration, soweit die Verknüpfung innerhalb der EDV-Abteilung geschieht,

- in der Mitteilung an die SAP-Administration, welche SAP-Konfigurationen wo vorhanden sind.

- Übermittlung personenbezogener Daten

Personenbezogene Daten der Beschäftigten im Rahmen dieser Betriebsvereinbarung dürfen nicht an andere externe Stellen außerhalb der Klinik Service GmbH übermittelt werden. Eine Ausnahme besteht in der Übermittlung an Hotline-Mitarbeiter der Firma Hermeskim, sofern diese nicht der Klinik Service GmbH angehören.

- Es erfolgen daher nur solche Verarbeitungen persönlicher Arbeitnehmerdaten, deren Zwecke vorher im Einzelnen festgelegt worden sind (Zweckbindung).

- Die Regeln der Verarbeitung müssen für alle Beteiligten klar erkennbar und nachvollziehbar sein (Normenklarheit).

- Die Verarbeitung persönlicher Arbeitnehmerdaten wird auf ein sparsames Ausmaß begrenzt: sie soll nur so viele Daten, wie zum Erreichen der jeweiligen Verarbeitungszwecke unbedingt erforderlich sind, umfassen (Verhältnismäßigkeit).

Der Einsatz eines SMARTPHONE ist nur dann zulässig, wenn folgende Sicherungsmaßnahmen durchgeführt wurden:

- Es ist täglich eine Datensicherung mithilfe einer Sicherungssoftware durchzuführen.
- Daten, die gelöscht werden sollen, müssen derart gelöscht werden, dass eine Wiedergewinnung ausgeschlossen ist.
- Personenbezogene Daten der Arbeitnehmer, die sich aus der Nutzung der mobilen Endgeräte ergeben (insbesondere Protokoll- und Verbindungsdaten) dürfen nur erhoben, gespeichert und genutzt werden, wenn dies zur Herstellung der Kommunikationsmöglichkeiten unvermeidbar ist.

- Ein Fernzugriff auf die mobilen Endgeräte ist ausschließlich zur Behebung technischer Probleme. Der Fernzugriff muss klar erkennbar sein und durch den Arbeitnehmer jederzeit auf einfachem Weg beendet werden können.
- Protokoll und Verbindungsdaten sind nach Ende des jeweiligen Kommunikationsvorgangs unverzüglich, spätestens aber nach 24 Stunden zu löschen, es sei denn, dass sich längere Speicherfristen aus zwingenden gesetzlichen Vorschriften ergeben.
- Der Kreis der Personen, die aus technischen Gründen auf Protokoll und Verbindungsdaten zugreifen können müssen, ist wie in Anlage 5.1, 5.2, 5.5, 5.6 festgelegt. SIEHE § 5, 6 und 7 (EDV, BR und Arbeitgeber im 6 Augen Prinzip)
- Überwachung des Verhaltens und/oder der Leistungen, die heimlich, das heißt nicht transparent offengelegt, angefertigt werden, bedürfen einer ausdrücklichen Gestattung durch die Betriebsparteien getroffene Einigung unter Beachtung des § 26 Abs. BDSG der AN und Anlage 5.5, 5.6
- Es darf kein GPS Tracking eingesetzt werden.
- Die zulässigen Datenverarbeitungen (Programme, Funktionen) werden gemeinsam mit dem Arbeitgeber in einer gesonderten § 5, 6, 7, 8) gemeinsam festgelegt. Jede Erweiterung oder Änderung sind mit dem BR in schriftlicher Form abzustimmen.
- Personaldaten, die nur für statistische Zwecke benötigt werden, sind unverzüglich zu anonymisieren.
- Protokolldateien werden nach 5 Tagen überschrieben und damit auch physikalisch gelöscht. Ausnahmen bedürfen der Vereinbarung.
- Personenbezogene oder personenbeziehbare Daten dürfen nicht zum Zweck einer Leistungs- und Verhaltenskontrolle herangezogen werden. Ausnahmen bedürfen einer besonderen Vereinbarung.
- Bei konkretem Verdacht des Verstoßes gegen den Datenschutz bzw. auf missbräuchliche Nutzung des SMARTPHONES kann unter vorheriger Beteiligung des Betriebsrates eine mitarbeiterbezogene Überprüfung von personenbezogenen Daten durchgeführt werden.
- Diese Überprüfung erfolgt durch den Kontrollausschuss, bestehend aus dem Betriebsrat, dem Datenschutzbeauftragten, einem Netzwerkadminstrator und einem Vertreter der Geschäftsführung. Der Sicherheitsausschuss hört die Betroffenen und fertigt einen Bericht an, der den Betroffenen, dem Betriebsrat und der Geschäftsführung weiterzuleiten ist. Der Bericht soll eine Empfehlung über das weitere Vorgehen enthalten.
- Es werden keine Programmfunktionen zur Verfügung gestellt, in denen Mitarbeiteridentifizierungen statistisch oder zeitlich zurückverfolgend ausgewertet werden, es sei denn, dies ist zwischen Arbeitgeber und Betriebsrat ausdrücklich vereinbart. Dies gilt auch für Auswertungen über das Benutzerverhalten kleiner Gruppen (20 oder weniger Personen).