Richtlinie Home-Office/Mobile-Office

§ 1 Gegenstand der Richtlinie, Allgemeines

(1) Diese Richtlinie regelt arbeitsrechtliche und datenschutzrechtliche Fragen sowie Fragen der Datensicherheit, wenn Mitarbeitern ein Arbeitsplatz in der eigenen Wohnung oder ein mobiler Arbeitsplatz (Home-Office/Mobile-Office – folgend zusammenfassend „Heimarbeitsplatz“) durch mbi zur Verfügung gestellt wird. Sie ergänzt die allgemeinen betrieblichen Bestimmungen zu Datenschutz und Datensicherheit, die auch am Heimarbeitsplatz stets einzuhalten sind. Im Fall von Widersprüchen geht diese Richtlinie vor.

(2) Diese Richtlinie begründet keinen Anspruch des Mitarbeiters auf die Zurverfügungstellung eines Heimarbeitsplatzes.

(3) Ein Heimarbeitsplatz darf nur zur Verfügung gestellt und genutzt werden, wenn die dort zu leistende Tätigkeit zur Erledigung außerhalb des Betriebs geeignet ist, insbesondere mit Blick auf Datenschutz- und Datensicherheitsaspekte.

(4) Ein Heimarbeitsplatz sollte nur zur Verfügung gestellt und genutzt werden, wenn der Mitarbeiter eine Schulung über Datenschutz und Datensicherheit bei Nutzung von Heimarbeitsplätzen absolviert hat, die in angemessenen Abständen zu wiederholen ist.

§ 2 Umgang mit Daten

(1) Auch, wenn Mitarbeiter an ihrem Heimarbeitsplatz tätig werden, bleiben sie Beschäftigte von mbi. Dies bedeutet, dass alle vertraglichen Weisungsrechte bestehen bleiben und insbesondere alle betrieblichen Daten, Informationen und Unterlagen, auf die Mitarbeiter von ihrem Heimarbeitsplatz aus Zugriff haben, ausschließlich im Hoheitsbereich von mbi bleiben. Allen Mitarbeitern ist es daher untersagt, betriebliche Daten, Informationen oder Unterlagen – insbesondere personenbezogene und sonst vertrauliche Daten – an Dritte weiterzugeben, sie Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken oder im Internet/Sozialen Medien), sie auf eigenen Speichermedien abzuspeichern, unbefugt zu kopieren oder zu anderen als betrieblichen Zwecken zu verwenden.

(2) Insbesondere

- ist es verboten, Dritten Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV (z. B. Chipkarten) mitzuteilen oder zugänglich zu machen, z. B. durch Notieren von Passwörtern oder Lagerung der Chipkarte am Lesegerät;
- ist es verboten, Dritten (z. B. Familienmitgliedern, sonstigen Mitbewohnern, Besuchern) Zugriff auf die betriebliche EDV und/oder betriebliche Unterlagen zu gewähren;
- ist es verboten, betriebliche Daten auf anderen Speichermedien als von mbi schriftlich zugelassen zu speichern; zugelassen ist die Speicherung auf betrieblichen Servern (Laufwerk F („Bereichsordner“) und Z („Mitarbeiterverzeichnis“)). Verboten ist somit insbesondere die Speicherung von betrieblichen Daten auf privaten Smartphones, USB-Sticks, Computern o. ä. sowie in Cloudspeichern außerhalb des Hoheitsbereichs von mbi;
- ist es verboten, dienstliche Daten mit privaten Geräten zu verarbeiten; dazu gehört auch der Abruf des dienstlichen E-Mail-Accounts mit einem privaten Computer, Smartphone o. ä.;

– ist es verboten, Sicherheitsmaßnahmen zu deaktivieren oder zu umgehen oder sonstige technische Veränderungen an den durch mbi zur Verfügung gestellten Geräten vorzunehmen. Software darf nur nach Absprache mit der IT-Abteilung installiert werden;

– müssen eventuelle Ausdrucke mit vertraulichen Informationen (z. B. personenbezogenen Daten) sicher vernichtet werden, wenn sie nicht mehr benötigt werden (Aktenvernichter).

(3) Alle Störungen oder Auffälligkeiten bei der EDV-Nutzung sind unverzüglich der IT-Abteilung zu melden.

(4) Die private Nutzung der für den Heimarbeitsplatz bereitgestellten betrieblichen Geräte bzw. Zugangsmöglichkeiten (insbesondere Computer und Internetzugang) ist verboten.

(5) mbi ist jederzeit berechtigt, vom Mitarbeiter die Herausgabe sämtlicher betrieblicher Daten, Unterlagen und Akten einschließlich sämtlicher Kopien zu verlangen; sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit herauszugeben. Der Mitarbeiter kann hiergegen kein Zurückbehaltungsrecht geltend machen.

§ 3 Sicherheitsmaßnahmen im Home-Office

(1) Der Raum, in dem sich der Heimarbeitsplatz des Mitarbeiters befindet, soll bei Nichtnutzung durch den Mitarbeiter sowie wenn Gäste (auch Handwerker) in seiner Wohnung sind, abgeschlossen werden. Dies gilt nicht, wenn der Mitarbeiter alle Unterlagen sowie Geräte und Datenträger, auf denen betriebliche Daten gespeichert sind, für Dritte unzugänglich und sicher in einem abgeschlossenen Schrank lagert. Halten sich Dritte am Heimarbeitsplatz auf (z. B. Handwerker, die hier arbeiten müssen), muss der Mitarbeiter sie jederzeit beobachten.

(2) Verlässt der Mitarbeiter seinen Heimarbeitsplatz (und sei es nur kurz, etwa zur Toilette), muss sichergestellt sein, dass kein Dritter auf betriebliche Daten oder Akten zugreifen kann. Dies bedeutet insbesondere, dass

– der verwendete Computer gesperrt werden muss, so dass bei Rückkehr zumindest die Eingabe des Passwortes erforderlich ist;

– Fenster verschlossen sein müssen, außer bei kurzzeitiger Abwesenheit, während der ein Eindringen realistischer Weise ausgeschlossen werden kann (z. B. 10. Stock und keine Möglichkeit, aus der Nachbarwohnung herüberzuklettern);

– bei Nutzung von Papier-Akten diese in einem Schrank einzuschließen sind oder der Heimarbeitsplatz-Raum abzuschließen ist; dies gilt nur dann nicht, wenn der Mitarbeiter alleine zu Hause ist und seinen Heimarbeitsplatz nur kurzzeitig verlässt;

– bei Verlassen der Wohnung ein gegebenenfalls genutztes Zugangsmedium (z. B. Chipkarte, Transponder) vom Computer entfernt werden muss und bei Nutzung von Papier-Akten diese in einem Schrank einzuschließen sind.

§ 4 Zusätzliche Sicherheitsmaßnahmen im Mobile-Office

Bei der Nutzung eines mobilen Arbeitsplatzes (Mobile-Office) außerhalb der Wohnung des Mitarbeiters gilt ergänzend zu den Regelungen in § 3:

(1) Der Mitarbeiter darf den mobilen Arbeitsplatz außerhalb eines verschlossenen Raums nicht – auch nicht kurzzeitig – unbeaufsichtigt lassen, wenn nicht eine Aufsicht durch einen anderen Mitarbeiter von mbi sichergestellt ist. Ausnahmsweise kann der Vorgesetzte Ausnahmen zulassen, wenn der mobile Arbeitsplatz an feste oder ausreichend große Gegenstände angeschlossen, eine ausreichende soziale Kontrolle sichergestellt, die Abwesenheit nur kurz ist und keine besonders vertraulichen Daten verarbeitet werden.

(2) Bevor der Mitarbeiter seine direkte Aufmerksamkeit vom mobilen Arbeitsplatz entfernt, ist der Computer zu sperren und sind alle Zugangsmedien (z. B. Chipkarte, Transponder) zu entfernen und sicher zu verwahren.

(3) Die mobile Nutzung von Akten bedarf der Zustimmung des Vorgesetzten.

(4) Die Mitnahme des mobilen Arbeitsplatzes ins Ausland bedarf der Zustimmung des Vorgesetzten und des betrieblichen Datenschutzbeauftragten, wenn nicht der betriebliche Datenschutzbeauftragte in Abstimmung mit der Geschäftsführung für sämtliche Ziel- und Transitländer eine allgemeine Freigabe erteilt hat.

§ 5 Sicherheitsmaßnahmen beim Transport und bei der Übertragung von Akten und Daten

(1) Jede Mitnahme betrieblicher Daten und Akten benötigt die vorherige Zustimmung des Vorgesetzten in Textform.

(2) Nimmt der Mitarbeiter betriebliche Akten mit, dürfen diese nur in verschlossenen Behältnissen transportiert werden (z. B. verschlossene Kiste, verschlossener Aktenkoffer). Der Mitarbeiter darf die Akten beim Transport zu keiner Zeit unbeaufsichtigt lassen.

(3) Nimmt der Mitarbeiter betriebliche Daten mit, muss der Datenträger mit einem von der IT-Abteilung freigegebenen Verfahren nach dem Stand der Technik verschlüsselt sein.

(4) Jede Datenübertragung zwischen dem Heimarbeitsplatz und dem Betrieb – einschließlich Terminal-Zugriff – muss nach dem Stand der Technik verschlüsselt sein. Hierfür trägt die IT-Abteilung Sorge.

(5) Zugriffe und Zugriffsversuche vom Heimarbeitsplatz werden von mbi protokolliert und regelmäßig ausgewertet. Diese Daten werden nur zur Missbrauchsentdeckung, -bekämpfung und -verfolgung verwendet und nicht zur Leistungs- oder Verhaltenskontrolle.

§ 6 Kontroll- und Zutrittsrechte zur Wohnung

(1) Der Mitarbeiter räumt folgenden Personen das Recht ein, zur Kontrolle des Heimarbeitsplatzes seine Wohnung zu betreten:

a) zur Kontrolle der Arbeitssicherheit einer von mbi hierfür gesondert beauftragten Person;

b) zur Kontrolle der Datensicherheit und der Einhaltung der Datenschutzbestimmungen dem betrieblichen Datenschutzbeauftragten oder einer anderen von mbi beauftragten, fachkundigen Person;

c) zur Einrichtung, Wartung, Reparatur, Änderung, Abholung der von mbi bereitgestellten Arbeitsmittel der IT-Abteilung bzw. sonstigen hierfür gesondert beauftragten Personen;

d) zu den gesetzlich vorgesehenen Kontrollen allen Behörden, die den Heimarbeitsplatz aufsuchen dürften, wenn sich dieser im Betrieb befände, beispielsweise der Datenschutz-Aufsichtsbehörde;

Das Zutrittsrecht ist auf den Heimarbeitsplatz (einschließlich zugehöriger Einrichtungen, etwa Telefonanschluss im Keller o. ä.) begrenzt und auf das unbedingt Erforderliche zu beschränken. Jeder Zutritt ist rechtzeitig im Voraus abzustimmen, wobei auf die Interessen des Mitarbeiters, wie beispielsweise Kinderbetreuung, Rücksicht zu nehmen ist, und auf Werktage zwischen 8:00 Uhr und 18:00 Uhr zu beschränken, es sei denn, aus besonderen Gründen ist ein sofortiger oder kurzfristiger Zutritt oder ein Zutritt zu einem bestimmten Termin unbedingt erforderlich. Im Fall des Zutrittsrechts nach S. 1 lit. d) (Behörden) richten sich eventuelle Abstimmungspflichten und Zeiten nach den Befugnissen der Behörde, die diese hätte, wenn sich der Heimarbeitsplatz im Betrieb befinden würde, und beschränken sich die Pflichten von mbi darauf, den Mitarbeiter unverzüglich zu informieren, sobald ihm der

Zutrittswunsch bekannt wird, und auf Wunsch des Mitarbeiters zur Behörde zu vermitteln, um einen anderen Termin zu vereinbaren.

(2) Die Erlaubnis zur Einrichtung und Nutzung des Heimarbeitsplatzes steht zudem unter der aufschiebenden Bedingung, dass (der Heimarbeitsplatz kann also erst eingerichtet werden, wenn) sämtliche Mitbewohner des Mitarbeiters die gleichen Zutrittsrechte einräumen. mbi kann jederzeit verlangen, dass der Mitarbeiter die Zustimmung aller Mitbewohner schriftlich nachweist.

(3) Widerruft der Mitarbeiter oder einer seiner Mitbewohner das Zutrittsrecht oder kommt ein neuer Mitbewohner hinzu, der nicht die Zutrittsrechte nach Abs. 1 einräumt, erlischt automatisch die Berechtigung des Mitarbeiters, den Heimarbeitsplatz zu nutzen. Der Mitarbeiter ist verpflichtet, dies sofort mbi anzuzeigen, sämtliche betrieblichen Akten und Datenträger sofort in den Betrieb zurückzubringen und seine Arbeitsleistung auf Wunsch von mbi im Betrieb zu erbringen.

(4) Widerruft der Mitarbeiter oder einer seiner Mitbewohner das Zutrittsrecht oder kommt ein neuer Mitbewohner hinzu, der nicht die gleichen Zutrittsrechte einräumt, kann mbi zudem verlangen, dass der Mitarbeiter unverzüglich sämtliche von mbi bereitgestellten Arbeitsmittel auf eigene Kosten in den Betrieb zurückbringt.

§ 7 Beendigung der Zurverfügungstellung

Das Unternehmen ist bei Vorliegen eines sachlichen Grundes berechtigt, die Zurverfügungstellung der Home-Office Möglichkeit, unter Berücksichtigung der Interessen des Arbeitnehmers, zu beenden. Ein sachlicher Grund liegt insbesondere in folgenden Fällen vor:

- Wiederholter Verstoß des Arbeitnehmers gegen die Home-Office Richtlinie, insbesondere bei einem Verstoß gegen § 4 und § 5 „Sicherheitsmaßnahmen“ sowie § 6 „Kontroll- und Zugriffsrechte zur Wohnung“;
- Aufnahme einer Nebentätigkeit des Arbeitnehmers;
- Betriebsbedingte Gründe, die eine Anwesenheit des Mitarbeiters im Unternehmen erfordern;
- Reduktion der regelmäßigen Arbeitszeit des Arbeitnehmers.

§ 8 Beendigung der Heimarbeitsplatz-Nutzung

(1) Enden die Berechtigung des Mitarbeiters zur Nutzung des Heimarbeitsplatzes oder das Arbeitsverhältnis oder wird der Mitarbeiter unwiderruflich von der Pflicht zur Arbeitsleistung freigestellt, hat der Mitarbeiter unaufgefordert unverzüglich sämtliche betrieblichen Zugangsmedien (z. B. Chipkarten, Transponder), Datenträger und Akten (einschließlich Kopien) in den Betrieb zurückzubringen und dem Vorgesetzten zu übergeben. Sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit zu übergeben.

(2) Der Mitarbeiter hat zudem die Abholung sämtlicher von mbi bereitgestellter Arbeitsmittel durch von mbi beauftragte Personen nach angemessener Ankündigungsfrist zu dulden.

§ 9 Hinweis auf rechtliche Folgen bei Verstößen

mbi weist darauf hin, dass Verstöße gegen diese Richtlinie nicht nur arbeitsrechtliche Folgen (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung) haben, sondern auch mit Geldbuße bedroht und/oder strafbar sein können (z. B. im Fall des Kopierens von Daten nach Art. 83 DS-GVO, § 42 BDSG, § 23 UWG, § 203 StGB). Darüber hinaus können Verstöße gegen diese Richtlinie Unterlassungs- und Schadensersatzansprüche nach sich ziehen.

Wetzlar, den 19.02.2024

_____

Mitarbeiter