© **FM Forum Business Solutions GmbH**
A-1200 Wien, Dresdner Straße 45
E-Mail: kundenservice@forum-media.at

BYOD

abgeschlossen zwischen der Geschäftsführung der Firma … und dem Betriebsrat der Firma …

Präambel

Im Regelfall werden für den dienstlichen Gebrauch auch dienstliche (IT-)Geräte verwendet. Aus praktischen Gesichtspunkten haben viele Mitarbeiter jedoch den Wunsch, private Hardware, insbesondere wie Smartphones, Tablets oder Laptops, auch für dienstliche Zwecke zu verwenden. Soll die Verwendung privater Hardware für dienstliche Zwecke zugelassen werden, bedarf es der Erfüllung der in dieser Vereinbarung genannten Voraussetzungen. Da die Nutzung privater Hardware zu dienstlichen Zwecken ein nicht zu unterschätzendes Sicherheitsrisiko für jedes Unternehmen darstellt, ist die Einhaltung der folgenden Bestimmungen unbedingt notwendig.

1. Allgemeines

1.1 Gegenstand
Gegenstand dieser Vereinbarung ist die Nutzung privater Hardware zu dienstlichen Zwecken.

1.2 Geltungsbereich
Diese Betriebsvereinbarung gilt für alle Dienstnehmer, die mit ihrem Dienstgeber die Nutzung privater Smartphones, Tablets oder Laptops (im Folgenden: private Hardware) zu dienstlichen Zwecken vereinbaren. Ohne den Abschluss einer solchen Vereinbarung unter Bezugnahme auf diese Betriebsvereinbarung ist die Nutzung privater Hardware für dienstliche Zwecke nicht gestattet.

1.3 Eine einzelvertragliche Vereinbarung über die Nutzung privater Hardware zu dienstlichen Zwecken bedarf der Schriftform.

1.4 Diese Betriebsvereinbarung begründet keinen Anspruch einzelner Dienstnehmer auf Aufnahme in das BYOD-Programm. Über die Aufnahme in das BYOD-Programm entscheidet der Dienstgeber auf Antrag der oder des einzelnen Dienstnehmer/s. Zwingende Voraussetzung für die Genehmigung des Antrags ist die Erfüllung der notwendigen technischen Voraussetzungen der jeweiligen privaten Hardware, um der Umsetzung der nachfolgenden Vorschriften für die dienstliche Nutzung zu entsprechen.

2. Zweck und Inhalt der Betriebsvereinbarung

2.1 Diese Betriebsvereinbarung regelt die Möglichkeit des Dienstnehmers, private Hardware zu dienstlichen Zwecken zu verwenden. Eine Aufnahme der oder des Mitarbeitenden in das BYOD-Programm begründet kein Telearbeitsverhältnis und keinen Anspruch auf einen Homeoffice-Arbeitsplatz. Sollten Regelungen zu Telearbeit, Homeoffice[1] oder Arbeits- und Gleitzeitregelungen bestehen, werden jene durch diese Betriebsvereinbarung nicht berührt und sind davon unabhängig zu beurteilen.

2.2 Ein Ersatz der durch den Dienstgeber zur Verfügung gestellten Betriebsmittel ist damit nicht verbunden.

2.3 Mit der Verwendung privater Hardware ist eine Leistungs- und Verhaltenskontrolle nicht verbunden.

3. Pflichten des Dienstgebers

3.1 Zu den Pflichten des Dienstgebers gehört die Zurverfügungstellung der notwendigen Infrastruktur, darunter versteht man einen Support-Dienst, der während der (Kern)Arbeitszeit bzw sofern eine solche nicht vorgesehen

ist, zu den jeweils vorgegebenen Dienstzeiten erreichbar ist. Dieser Supportdienst bietet Unterstützung bei der Bedienung der vom Dienstgeber zur Verfügung gestellten Applikationen und Programme.

3.2 Für den Zugang zu dienstlichen Daten wird ein „Mobile-Device-Management-System“[2] zur Verfügung gestellt. Soweit personenbezogene Daten von der Datenverarbeitung umfasst sind, ist auf die diesbezüglichen gesetzlichen Bestimmungen der Datenschutzgrundverordnung (DSGVO) bzw des Datenschutzgesetzes (DSG) zu verweisen.[3]

3.3 Das Mobile-Device-Management-System wird zu folgenden Zwecken eingesetzt:

- Management der dienstlichen Daten und Programme
- Überwachung der Einhaltung der IT-Sicherheitsstandards
- Überwachung der Einhaltung des Datenschutzes

3.4 Zur Sicherstellung der Einhaltung technischer und rechtlicher Anforderungen werden vom Dienstgeber die technischen Eigenschaften der jeweiligen privaten Hardware geprüft und registriert.

3.5 Der Betriebsrat erhält eine jeweils aktuelle Liste aller Dienstnehmer, die dem BYOD-Programm unterliegen.

4. Pflichten des Dienstnehmers

4.1 Jeder Dienstnehmer haftet für alle Rechtsverletzungen, welche unter Verwendung der jeweiligen privaten Hardware begangen werden, darunter versteht man auch Lizenz- und/oder Urheberrechtsverletzungen. Vor Aufnahme in das Programm hat jeder Dienstnehmer eine Überprüfung vorzunehmen, ob die auf der privaten Hardware installierte Software mit den jeweiligen Datenschutzbestimmungen konform ist.

4.2 Jeden Dienstnehmer trifft die Verpflichtung, den Dienstgeber bei IT-Sicherheitsvorfällen, Verlust oder Beschädigung der privaten Hardware unverzüglich zu informieren.

4.3 Die von dem Dienstnehmer verwendeten Applikationen sind vor Aufnahme in das Programm dahingehend zu prüfen, dass datenschutzrechtliche Standards eingehalten werden können.

4.4 Nach der Bearbeitung von Daten ist sicherzustellen, dass eine aktuelle Version auf dem Server des Dienstgebers gespeichert ist.

4.5 Der Dienstnehmer wird vor Installation eines Programmes, mit dem auf die dienstlichen Daten der privaten Hardware zugegriffen werden kann, eine entsprechende ausdrückliche Einwilligung erklären, ohne welche die Verwendung privater Hardware nicht möglich ist. Eine solche Kontrolle erfolgt ausschließlich zu dem Zweck, unberechtigte Zugriffe auf die Daten und Anwendungen zu identifizieren oder festzustellen, ob sich auf der privaten Hardware Schadprogramme befinden. Ein Echtzeit-/Remotezugriff erfolgt ausschließlich nach Beiziehen des Betriebsrats und jeweiliger Zustimmung des Dienstnehmers.

4.6 Jeder Dienstnehmer verpflichtet sich dazu, darauf zu achten, dass über andere Schnittstellen oder Programme (Bluetooth, USB, Cloud-Dienste etc) kein Zugriff auf dienstliche Daten genommen werden kann.

4.7 Während der Teilnahme am BYOD-Programm ist die Nutzung der privaten Hardware durch Dritte ausnahmslos unzulässig.

4.8 Das Prüfungs- und Kontrollrecht der oder des Datenschutzbeauftragten umfasst auch private Hardware.

5. Verwaltung der Daten auf der privaten Hardware

5.1 Jeder Dienstnehmer ist verpflichtet, den Anweisungen des Mobile Device Management-Systems Folge zu leisten. Dies umfasst insbesondere die Verpflichtung, notwendige Software zu installieren sowie Updates vorzunehmen und keine Löschung der diesbezüglichen Software ohne vorherige Zustimmung des Dienstgebers vorzunehmen.

5.2 Die Verwaltung von privaten und dienstlichen Daten hat getrennt zu erfolgen. Der Dienstnehmer hat darauf zu achten, dass eine Vermischung von dienstlichen und privaten Daten nicht vorgenommen werden kann. Der

Dienstgeber hat das Mobile Device Management-System so zu konfigurieren, dass eine Vermischung von dienstlichen und privaten Daten im Rahmen des technisch Möglichen vermieden wird. Die Erstellung von Sicherungskopien dienstlicher Daten außerhalb des Betriebsnetzwerks ist in jeglicher Form untersagt.

6. Kostentragung, Haftung

6.1 Alle in Zusammenhang mit der Anschaffung oder dem Betrieb der privaten Hardware anfallenden Kosten hat der Dienstnehmer selber zu tragen. Dazu zählen insbesondere die Kosten für die Anschaffung des Gerätes sowie dessen Zubehör und Anwendungen, soweit diese nicht vom Dienstgeber zur Verfügung zu stellen sind, sowie sämtliche Kosten, die für die Nutzung des Gerätes entstehen.

6.2 Es besteht keine Haftung des Dienstgebers für Verlust oder Beschädigung der privaten Hardware; dies gilt insbesondere für installierte Anwendungen, private Daten oder sonstige Inhalte.

6.3 Den Dienstnehmer trifft die Verpflichtung zum Ersatz aller im Zusammenhang mit der Verwendung der privaten Hardware entstehender Schäden, dies betrifft insbesondere Schäden aus Datenschutzverletzungen.

7. Sicherheitsanforderungen

7.1 Der Dienstnehmer verpflichtet sich, jegliche Sicherheitsanweisungen des Dienstgebers zu beachten und umgehend umzusetzen.

7.2 Der Dienstnehmer verpflichtet sich, seine private Hardware stets mit dem aktuellsten Virenschutzprogramm auszustatten.

7.3 Bei der Verwendung von Software achtet der Dienstnehmer besonders auf die Erfüllung des Sicherheitsstandards und zeigt jeglichen Verdachtsmoment auf unseriöse Quellen dem Dienstgeber unverzüglich an.

7.4 Der Dienstnehmer billigt in die Installation von Programmen ein, die eine Sperrung der privaten Hardware sowie die Fernlöschung von betrieblichen Daten ermöglicht, sofern dies dem Schutz betrieblicher Daten dient.

Eine Fernlöschung ist insbesondere in folgenden Fällen zulässig:

- Bei Beschädigung oder Diebstahl der privaten Hardware
- Bei zu häufiger Fehleingabe des PINs/Passwortes
- Bei Beendigung des BYOD-Programms
- Bei Beendigung des Dienstverhältnisses
- Bei schwerwiegendem Verstoß des Dienstnehmers gegen seine Pflichten hierunter
- Bei sonstigen Verstößen gegen rechtlich zwingende Vorgaben, insbesondere datenschutzrechtliche Verpflichtungen

7.5 Eine solche Fernlöschung ist dem Dienstnehmer vor deren Vornahme unverzüglich mitzuteilen, sodass dieser eine Sicherung seiner privaten Daten rechtzeitig vornehmen kann. Kommt es im Zuge einer solchen Fernlöschung von Daten zum Verlust privater Daten oder Inhalte, trifft den Dienstgeber in diesem Zusammenhang keine Haftung.

8. Beendigung der Teilnahme am BYOD-Programm

8.1 Eine Beendigung an der Teilnahme am BYOD-Programm durch den Dienstnehmer kann jederzeit ohne Angabe von Gründen erfolgen und bedarf der Schriftform.

8.2 Der Dienstgeber verpflichtet sich, jegliche im Zusammenhang mit der Teilnahme am BYOD-Programm erhaltenen Daten, die die jeweilige private Hardware betreffen, unverzüglich nach dem schriftlichen Zugang der Beendigung durch den Dienstnehmer zu löschen. Der Dienstnehmer hat im Fall des Ausscheidens aus dem

BYOD-Programm sämtliche dienstlichen Daten und Kontakte von seiner jeweiligen privaten Hardware auf den Server des Dienstgebers zu überspielen, sofern nicht eine automatische Synchronisation erfolgt. Anschließend sind diese Daten von seiner jeweiligen privaten Hardware unwiederbringlich zu löschen.

8.3 Der Dienstgeber kann die Teilnahme an dem BYOD-Programm in schriftlicher Form widerrufen, wenn der Dienstnehmer durch den Einsatz seiner privaten Hardware eine Datenschutzgefährdung darstellt oder sonstige wichtige Gründe vorliegen.

8.4 Die Teilnahme am BYOD-Programm endet jedenfalls mit Beendigung des jeweiligen Dienstverhältnisses. In diesem Fall gilt 8.2.

9. Geltungsdauer

9.1 Die Vereinbarung tritt am Tage der Unterzeichnung in Kraft und endet am … ohne Nachwirkung.

…, am …

…
Dienstgeber

…
Betriebsrat

Anmerkungen:

1 Hinweis auf rechtliche Änderungen „Homeoffice-Gesetz“ (Arbeitsvertragsrechts-Anpassungsgesetz, Arbeitsverfassungsgesetz ua, Änderung [94/ME]).

Zurück

2 Mobile Device Management (MDM) ist die zentralisierte Verwaltung von mobilen Geräten wie Smartphones, Tablets und Notebooks im Unternehmen. MDM beabsichtigt bei gleichzeitigem Schutz des Unternehmensnetzwerks die Sicherheit und Funktionalität dieser Geräte am Arbeitsplatz zu optimieren.

Zurück

3 Wichtig hier vor allem bestehende Informationspflichten über die Art und die Dauer der personenbezogenen Datenverarbeitung.

Zurück