Empfehlung: Bitte beachten Sie, dass dieses Dokument als Mustervorlage dienen soll und an die entsprechenden Gegebenheiten in Ihrem Unternehmen angepasst werden muss. Wir empfehlen dazu die Abstimmung mit entsprechenden involvierten Parteien, wie z. B. Personalabteilung, IT-Abteilung, Recht/Compliance-Abteilung, Betriebsrat etc. Außerdem möchten wir Sie darauf hinweisen, dass die Verwendung dieser Vorlage keine rechtliche Beratung ersetzt und die Nutzungsvereinbarung abschließend einer rechtlichen Prüfung unterzogen werden sollte.

[MUSTER] BRING YOUR OWN DEVICE (BYOD) POLICY

POLICY ZUM THEMA BRING YOUR OWN DEVICE (BYOD), ALSO DER DIENSTLICHEN NUTZUNG PRIVATER ENDGERÄTE.

Arbeitgeber und Verantwortlicher im Sinne dieser Policy ist **[Firmenname]**.

§ 1 NUTZUNG PRIVATER ENDGERÄTE

Dem Arbeitnehmer ist es gestattet, zur betriebsinternen, aber auch zur externen Kommunikation eigene, mobile private Endgeräte wie Smartphone und Tablet-Computer dienstlich zu nutzen. Die Nutzung des privaten Endgerätes für dienstliche Zwecke erfolgt auf Wunsch des Arbeitnehmers. Falls der Arbeitnehmer dies jetzt oder künftig nicht mehr wünscht, stellt der Arbeitgeber ihm die für seine Arbeit notwendigen Endgeräte zur Verfügung.

§ 2 ARBEITGEBER ALS VERANTWORTLICHE STELLE, TECHNISCHE UND ORGANISATORISCHE SICHERHEITS-MASSNAHMEN

Werden bei der Nutzung der privaten Endgeräte personenbezogene Daten, die im Zusammenhang mit der dienstlichen Tätigkeit stehen, auf privaten Endgeräten verarbeitet, bleibt der Arbeitgeber dennoch Verantwortlicher im Sinne des Datenschutzrechts. Der Arbeitgeber hat deshalb die Möglichkeit, gewisse Mindestanforderungen an Hardware, Betriebssystem und Schutzeinrichtungen zu stellen, um das Funktionieren von Systemen und Anwendungen auf Unternehmensseite zu gewährleisten, und die technischen und organisatorischen Maßnahmen auf den privaten Endgeräten zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. **[Definition von Mindestanforderungen.]** Die seitens der IT-Abteilung des Arbeitgebers vorgegebenen technischen und organisatorischen Maßnahmen, werden von der IT-Abteilung des Arbeitgebers auf den privaten Endgeräten administriert. Zur Verfügung gestellte Aktualisierungen (vor allem Sicherheitsupdates) müssen vom Arbeitnehmer unverzüglich auf seinem privaten Endgerät installiert werden. **[Definition der zugelassenen Applikationen; z.B. „Für die dienstliche Kommunikation sind auf den mobilen privaten Endgeräten ausschließlich „SecurePIM“ und zugehörige Companion-Apps zu benutzen.“].** Für die Verarbeitung und Sicherung privater Daten hat der Arbeitnehmer eigenverantwortlich Sorge zu tragen.

§ 3 DATENSCHUTZGRUNDSÄTZE

Zwischen privaten und geschäftlichen Daten ist zu trennen. Dazu sind betriebsbezogene Daten in einem separaten Speicher abzulegen, der z.B. über einen Datencontainer geschützt wird. Der Datencontainer muss mit einem Passwort (nach Maßgabe der Passwortrichtlinie des Arbeitgebers) geschützt werden und der Passwortschutz muss immer aktiv sein, wenn der Arbeitnehmer das Endgerät nicht verwendet. Der Arbeitnehmer muss sicherstellen, dass sämtliche betriebsbezogenen Daten aus dem lokalen Container ggf. auch zeitnah auf das Firmenlaufwerk übertragen werden.

Außerhalb des Containers dürfen keine personenbezogenen Daten firmenrelevanter Kundenkontakte gespeichert werden, d.h. das Speichern der Kundenkontakte in der normalen Kontaktliste des Mobiltelefons ist nicht gestattet. Ebenso dürfen keine privaten Daten im separaten Container für die Firmendaten gespeichert werden. Bevor der Arbeitnehmer sein privates Endgerät Dritten (einschließlich Kolleginnen bzw. Kollegen und Familienangehörigen) zur Verfügung stellt muss der Container geschlossen werden.

Für den Fall des Verlustes, des Diebstahls, der Zerstörung, der dauerhaften Überlassung an einen Dritten oder der Pfändung seines privaten Endgerätes hat der Arbeitnehmer unverzüglich, spätestens innerhalb von 24 Stunden (auch an Wochenenden) die IT-Abteilung des Arbeitgebers zu unterrichten und mitzuteilen, ob aufgrund dieses Ereignisses die Gefahr der Verletzung des Schutzes personenbezogener Daten besteht. Es erfolgt sodann die Fernlöschung des Datencontainers durch die IT-Abteilung des Arbeitgebers.

§ 4 STRAFRECHTLICHER SCHUTZ

Es besteht ein strafrechtlicher Schutz von unternehmensbezogenen Daten und Geschäfts- und Betriebsgeheimnissen durch § 17 UWG. Ein Geschäfts- oder Betriebsgeheimnis ist jede im Zusammenhang mit dem Betrieb des Arbeitgebers stehende, nicht offenkundige, sondern nur einem eng begrenzten Personenkreis bekannte Tatsache, an deren Geheimhaltung der Unternehmensinhaber ein berechtigtes, wirtschaftliches Interesse hat und die nach seinem bekundeten oder doch erkennbaren Willen auch geheim bleiben soll.

§ 5 ZUGRIFFSREGELUNG

Der Arbeitnehmer muss dem Arbeitgeber auf Aufforderung Zugriff zu den betriebsbezogenen Daten auf dem privaten Endgerät gewähren und diese dem Arbeitgeber zur Verfügung stellen. Wird das Arbeitsverhältnis beendet, verpflichtet sich der Arbeitnehmer, dem Arbeitgeber alle betriebsbezogenen Daten zur Verfügung zu stellen und diese sodann auf dem privaten Endgerät zu löschen.

§ 6 ARBEITSZEIT

[Regelung zur Benutzung des privaten Endgerätes für dienstliche Zwecke während der Ruhezeiten bzw. außerhalb der Arbeitszeiten.]

§ 7 KOSTEN

[Regelung zur Kostenübernahme durch den Arbeitgeber, z.B. für Verbindungskosten oder Hardwarekosten.]

§ 8 WIDERRUF DER POLICY

Die Gestattung der dienstlichen Nutzung privater Endgeräte erfolgt durch den Arbeitgeber freiwillig und ohne Rechtsanspruch des Arbeitnehmers hierauf. Der Arbeitgeber behält sich vor, diese Policy mit Wirkung für die Zukunft zu widerrufen und die dienstliche Nutzung privater Endgeräte zu untersagen.

§ 9 SALVATORISCHE KLAUSEL

Sollten einzelne Bestimmungen dieser Policy unwirksam sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen dieser Policy nicht berührt.

§ 10 INKRAFTTRETEN

Diese Policy tritt am Tag der Unterzeichnung in Kraft.

Ich habe diese Policy zur Kenntnis genommen und erkläre mich damit einverstanden.

_____

Ort, Datum, Unterschrift - Arbeitnehmer