

MUSTERVORLAGE PRIVATE NUTZUNG DIENSTLICHER ENDGERÄTE

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.

BETRIEBSVEREINBARUNG ZUR PRIVATEN NUTZUNG DIENSTLICHER ENDGERÄTE MIT DER CONTAINER APP SECUREPIM.

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

§ 1 ÜBERLASSUNG EINES SMARTPHONES

Der Arbeitgeber überlässt dem Arbeitnehmer ein Smartphone inkl. Zubehör [Marke/Typ des Handys und des ausgegebenen Zubehörs] mit der SIM-Karte Nr. _____.

Der Vertrag über das Mobiltelefon wird zwischen dem Arbeitgeber und dem Mobilfunkbetreiber geschlossen. Der Arbeitgeber behält sich das Recht vor, das Smartphone mit einer Ankündigungsfrist von _____ entschädigungsfrei zurückzufordern.

§ 2 RÜCKGABE DES SMARTPHONES

Der Arbeitnehmer verpflichtet sich bei Beendigung des Arbeitsverhältnisses durch den Arbeitnehmer oder den Arbeitgeber (z.B. bei Kündigung, Aufhebungsvertrag usw.) das Smartphone unaufgefordert dem Arbeitgeber unverzüglich zurückzugeben (inkl. des erhaltenen Zubehörs).

Der Arbeitgeber kann jederzeit die Rückgabe des dienstlichen Smartphones inkl. Zubehör verlangen.

§ 3 DATENSCHUTZGRUNDSÄTZE

Betriebsbezogene Daten sind in einem separaten Speicher abzulegen, der über einen SecurePIM 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 SecurePIM Container ggf. auch zeitnah auf das Firmenlaufwerk übertragen werden. Eine Übertragung oder Speicherung von Daten aus dem lokalen SecurePIM Container auf Speichereinrichtungen, Speichermedien oder in Cloud-Diensten (z.B. Dropbox, Google Drive oder iCloud) ist nur zulässig, falls diese vom Arbeitgeber ausdrücklich zur dienstlichen Nutzung freigegeben wurden.

Es ist untersagt, das Smartphone und/oder die SIM-Karte an Dritte weiterzugeben, Dritten zugänglich zu machen oder an Dritte zu verleihen. Das Smartphone ist mit einer Codesperre zu sichern. Die PIN-Nummer ist geheim zu halten.

Vor Rückgabe des Smartphones an das Unternehmen ist der Arbeitnehmer verpflichtet alle eventuell vorhandenen privaten Daten vom dienstlichen Smartphone zu löschen.

§ 4 SCHUTZMASSNAHMEN

Die seitens der IT-Abteilung vorgegebenen Schutzmaßnahmen dürfen nicht deaktiviert oder auf sonstige Weise außer Betrieb gesetzt oder umgangen werden.

Zur Verfügung gestellte Aktualisierungen müssen vom Arbeitnehmer unverzüglich auf seinem Endgerät installiert oder das Smartphone der IT-Abteilung zur Durchführung dieser Arbeiten überlassen werden.

MUSTERVORLAGE PRIVATE NUTZUNG DIENSTLICHER ENDGERÄTE

Der Arbeitnehmer darf nur vom Arbeitgeber freigegebene Anwendungen und autorisierte Programme auf dem Smartphone installieren. Etwaige Kosten und Schäden, die bei der Installation und Nutzung von unerlaubten Anwendungen entstehen, gehen zu Lasten des Arbeitnehmers.

Für die dienstliche Kommunikation und Bearbeitung von dienstlichen Dokumenten ist auf den mobilen Geräten ausschließlich SecurePIM und zugehörige Companion-Apps zu benutzen.

Personenbezogene Daten von Kunden, Kollegen oder Geschäftspartnern dürfen nicht außerhalb des Containers bearbeitet oder gespeichert werden. Der Zugangscod zur App ist gemäß der Passwortrichtlinie des Arbeitgebers zu wählen und geheim zu halten.

§ 5 UMGANG MIT DEM DIENSTLICHEN SMARTPHONE

Der Besitzer eines dienstlichen Smartphones muss sorgfältig mit diesem umgehen. Er muss dafür sorgen, dass er es stets sicher verwahrt. Bei Verlust, Diebstahl oder Beschädigung 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.

Der Arbeitnehmer haftet für alle Schäden, die von ihm grob fahrlässig oder vorsätzlich verursacht wurden.

§ 6 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.

§ 7 ARBEITSZEIT

Der Arbeitnehmer ist außerhalb seiner vertraglich vereinbarten Arbeitszeit weder verpflichtet, dienstliche Gespräche auf seinem privaten Endgerät anzunehmen oder dienstliche E-Mails abzurufen und zu lesen oder zu bearbeiten, noch erwartet der Arbeitgeber dies. Auch sollen am Wochenende keine dienstlichen Arbeiten über das private Endgerät erledigt werden. Gleiches gilt für Feiertage und die Dauer des Urlaubs.

§ 8 KOSTEN

Die Anschaffungskosten und die laufenden Kosten für das Gerät trägt vollständig der Arbeitgeber. Die mit der Nutzung des Smartphones verbundenen Verbindungskosten trägt grundsätzlich der Arbeitgeber. Der Arbeitnehmer hat darauf zu achten die jeweils kostengünstigere Variante für E-Mail, Internet, Telefon usw. zu nutzen (z.B. kostenfreies WLAN, Festnetz). Dies gilt insbesondere bei Kontakten ins Ausland und auf Dienstreisen.

§ 9 NUTZUNG BEI AUSLANDSAUFENTHALTEN

Bei Auslandsaufenthalten außerhalb von EU-Mitgliedsstaaten sollte die Datenübertragung (E-Mail, Internet, Push-Nachrichten) grundsätzlich über WLAN erfolgen und das Datenroaming deaktiviert sein.

§ 10 NUTZUNG

Das Smartphone dient der betrieblichen Nutzung (Telefonie, E-Mail, Internet) durch den Arbeitnehmer. Der Arbeitgeber gestattet eine private Nutzung des Smartphones durch den Arbeitnehmer im Rahmen des abgeschlossenen Tarifes, d. h. sofern entstehende Kosten der privaten Nutzung als unwesentlich (10:90 Relation) anzusehen sind.

Der Arbeitgeber behält sich den jederzeitigen Widerruf der privaten Nutzung vor.

§ 11 SALVATORISCHE KLAUSEL

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

§ 12 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