

Checkliste

17 nützliche Tipps, wenn Ihre Mitarbeiter:innen Handys beruflich UND privat nutzen

Immer mehr Unternehmen stellen ihren Mitarbeiter:innen Smartphones und Tablets zur Verfügung und erlauben ihnen neben der beruflichen auch die private Nutzung der Geräte. Dieses Modell nennt sich COPE (Corporate Owned Personally Enabled). Es gibt aber auch immer mehr Firmen, in denen Mitarbeiter:innen gegen eine Kostenbeteiligung ihre privaten Geräte auch beruflich nutzen. BYOD (Bring Your Own Device) nennt sich dieses Modell.

Die Vorteile des COPE- bzw. BYOD-Modells für den/die Mitarbeiter:in liegen auf der Hand:

Die Mitarbeiter:innen müssen nur ein Gerät mit sich herumtragen. Außerdem haben sie keine oder geringere Kosten für die Anschaffung eines Gerätes. Ein besonderes Highlight für Mitarbeiter:innen ist, wenn die Geräte vom Unternehmen gestellt werden und der/die Mitarbeiter:in sich dieses Gerät auch noch selbst aussuchen darf (CYOD – Choose your own device).

Allen drei Bereitstellungsmodellen ist eines gemeinsam: Wenn Sie Ihren Mitarbeiter:innen Firmenhandys bereitstellen und ihnen die private Nutzung erlauben oder wenn private Geräte auch beruflich genutzt werden, sollten Sie einige Dinge unbedingt beachten, um Streitereien und Problemen vorzubeugen.

Die wichtigste technische Voraussetzung für ein funktionierendes COPE oder BYOD ist der Einsatz eines Mobile-Device-Management-Systems MDM. Bei einer gleichzeitig geschäftlichen wie privaten Nutzung auf einem Gerät müssen die beruflichen und die privaten Daten sauber voneinander getrennt bleiben. Andernfalls kommt es schnell zu einem Verstoß gegen die Datenschutz-Grundverordnung DSGVO. Diese saubere Trennung ist nur beim Einsatz eines MDM vollumfänglich möglich.

Folgen Sie einfach den 17 Tipps aus unserer Checkliste, damit sowohl Sie als auch Ihre Mitarbeiter:innen vom COPE- oder BYOD-Modell profitieren.

Beachten Sie diese 17 Hinweise!

1. Stellen Sie sicher, dass die Smartphones und Tablets die technischen Voraussetzungen, die von der IT-Abteilung gefordert werden, erfüllen.
2. Führen Sie unbedingt eine MDM-Lösung zur datenschutzkonformen Verwaltung der Geräte ein, falls noch nicht vorhanden.
3. Erklären Sie den Mitarbeiter:innen, dass die IT-Administrator:innen im Notfall entfernt auf ihr Gerät zugreifen können, jedoch nur auf den abgeschotteten Bereich mit den geschäftlichen Daten. Die privaten Daten sind vor dem Zugriff seitens des Arbeitsgebers sicher.
4. Machen Sie den Mitarbeiter:innen deutlich, dass sie das Handy mit einem starken, langen und komplexen Passwort schützen müssen.
5. Erklären Sie, dass das Endgerät lokalisiert werden kann, z.B. wenn es verloren ging oder gestohlen wurde. Dies funktioniert jedoch nur, wenn die Ortungsdienste für das Arbeitsprofil aktiviert sind (nur Android).
6. Erklären Sie ihnen außerdem, dass der geschäftliche Bereich – aber nicht der private Bereich – inkl. aller Apps und Daten von dem Gerät gelöscht werden kann (Partial Wipe). In keinem Fall werden private Daten, wie z.B. Bilder gelöscht.
7. Machen Sie deutlich, dass Sie als Arbeitgeber alle auf dem Endgerät installierten geschäftlichen Apps einsehen können. Aber dies ist ja auch bei allen anderen Firmenrechnern selbstverständlich der Fall.
8. Schärfen Sie Ihren Mitarbeiter:innen ein, dass nur sie selbst, auf keinen Fall aber Familienmitglieder, Freunde oder andere Firmenfremde Zugriff auf den Bereich mit den Firmendaten haben dürfen.
9. Betonen Sie, wie wichtig es ist, dass das Gerät über das MDM verwaltet wird. Andernfalls besteht ein Sicherheitsrisiko für die Firma. Sie müssten sich dann vorbehalten, das Gerät zurückzufordern, bzw. die berufliche Nutzung des privaten Gerätes zu untersagen.
10. Weisen Sie darauf hin, dass der:die Mitarbeiter:in sich durch das Handy oder Tablet nicht verleiten lassen soll, die vorgeschriebene Regelarbeitszeit von durchschnittlich 8 bis maximal 10 Arbeitsstunden/Werktag gem. § 3 ArbZG zu überschreiten.
11. Machen Sie dem:der Arbeitnehmer:in klar, dass er:sie Ihnen den Verlust oder Defekt des Endgerätes unverzüglich mitteilen muss. Mit einer schnellen Reaktion im Verlustfall können Firmendaten verlässlich geschützt werden.
12. Empfehlen Sie dem:der Arbeitnehmer:in, in regelmäßigen Abständen Sicherungen des Endgeräts vorzunehmen.

- 13.** Eigentlich selbstverständlich: Handelt es sich um ein Firmengerät, müssen alle sich auf dem Endgerät befindlichen geschäftlichen Daten ebenso wie das Endgerät selbst bei einer Beendigung des Beschäftigungsverhältnisses oder auch bei Beendigung der Teilnahme an COPE/CYOD-Programm abgegeben werden. Auf BYOD-Geräten müssen in diesen Fällen alle geschäftlichen Daten gelöscht werden.
- 14.** Bei der Nutzung von Apps sollten Sie sich mit dem/der Mitarbeiter.in verständigen. Sollen private Apps auch geschäftlich genutzt werden oder umgekehrt geschäftliche auch privat, dann müssen Sie die Lizenzbedingungen prüfen und Kosten ggf. untereinander aufteilen.
- 15.** Der/die Arbeitnehmer.in sollte seine privaten Daten wie z.B. Kontakte, Fotos und Musik nicht im Zusammenhang mit seiner geschäftlichen Tätigkeit verwenden.
- 16.** Anders herum dürfen Firmendaten, wie z.B. geschäftliche Kontakte nicht in das private Adressbuch des/der Arbeitnehmers.in übernommen werden.
- 17.** Falls das Gerät mit einem Firmenvertrag läuft, klären Sie mit dem/der Arbeitnehmer.in, dass die Roamingkosten bei der privaten Verwendung des Endgerätes im Nicht-EU-Ausland einen festgelegten Betrag, z.B. 50 Euro pro Monat nicht übersteigen sollen.

Sie wollen Cortado MDM kostenlos und unverbindlich testen? Dann nutzen Sie gern unseren [Demo-Link](#)

Sie interessieren sich für Firmenhandys inklusive MDM und würden die Beschaffung und Einrichtung der Geräte lieber gleich in kompetente Hände legen? Dann machen wir Ihnen gern ein [Angebot](#).

