# Leitfaden für die Nutzungsrichtlinien bei der Realisierung von Mobile Device Management

**Vorschläge und Beachtenswertes**

**Ihr Ansprechpartner:**


Walter Hofmann

*Cloud Director COMPAREX AG*

email: walter.hofmann@comparex.de

mobile: +49 172 8559036





**COMPAREX AG**
Blochstraße 1, 04329 Leipzig
phone: +49 341 2568 000
fax: +49 341 2568 999
email: info@comparex.de
website: www.comparex.de
Amtsgericht Leipzig: HRB 15064

**Vorstand:**
Hansjörg Egger (Vorstandsvorsitzender)
Dr. Thomas Reich
Lilienbrunngasse 7-9, A-1020 Wien
Vorsitzender des Aufsichtsrates:
Wilfried Pruschak
Steuer-Nr.: 232/100/00704
USt-IdNr.: DE 141626867

**Bankverbindungen:**
**Deutsche Bank AG**
KTO: 11 74 960 00
BLZ: 860 700 00 • IBAN:
DE 75 8607 0000 0117 4960 00
(EUR/USD/CHF/GBP)
SWIFT/BIC: DEUTDE8L

**Commerzbank AG**
KTO: 12 48 960 00
BLZ: 860 800 00 • IBAN:
DE 20 8608 0000 0124 8960 00
(EUR/USD)
SWIFT/BIC: DRESDEFF860

**UniCredit Bank AG - HypoVereinsbank**
KTO: 67 19 279
BLZ: 860 200 86 • IBAN:
DE 93 8602 0086 0006 7192 79
(EUR)
SWIFT/BIC: HYVEDEMM495

# Inhalt

# 1 Auf die richtige Vorbereitung kommt es an

Das Marktforschungs- und Beratungsinstitut Gartner prognostiziert, dass 9 von 10 Unternehmen in Deutschland bis 2017 eine Mobile-Device-Management-Lösung einführen oder eine solche bis dahin eingeführt haben werden. In allen Projekten werden COMPAREX-Experten gefragt, auf welche Details man bei der Erstellung und Ausprägung der Nutzungsrichtlinien (Policies) denn genau achten sollte.

Aus diesem Grund wurde dieses Dokument als Leitfaden entwickelt. Nutzen Sie es, um sich selbst im Vorfeld die richtigen Fragen zu stellen und sich damit intensiv auf die spätere Umsetzung vorbereiten zu können.

Nur die gesammelten Informationen aus den Bereichen IT, Personalabteilung (HR) und ggf. dem Betriebsrat können am Ende eine belastbare Richtlinie für eine praktikable MDM-Lösung ergeben. Bitte beachten sie, dass dieses Dokument nur die Vorarbeit für einen späteren Implementierungs-Workshop liefern kann. In vielen Fällen hat dieses Dokument bereits im Vorfeld für eine bessere Strukturierung und Klarheit der umzusetzenden Nutzungsrichtlinie (Policy) geführt, so dass spätere Aufwände deutlich reduziert werden konnten.

Dieses Dokument hat keinen Anspruch auf Vollständigkeit der Fragen und stellt kein verbindliches Angebot dar, sondern dient ausschließlich der intensiven Vorbereitung.

## 1.1 Sieben Schritte zum Erfolg

**Schritt 1: Mobility-Strategie**

Zunächst muss sich jedes Unternehmen klar darüber werden, welche Rolle das Thema Mobilität generell einnimmt und inwiefern MDM in eine generelle Arbeitsplatz-Strategie eingebettet werden kann und soll. Um auch zukünftige Anforderungen in die Planung mit einzubeziehen, ist eine vorausschauende Einschätzung zur Entwicklung des Themas sinnvoll (Ziele, spezielle Bedürfnisse, aktueller Status, Erstausbau usw.). Bitte beschreiben Sie in mindestens 5 Sätzen diesen Sachverhalt.

**Schritt 2: BYOD (Bring Your Own Device) oder Firmengeräte**

Dürfen Mitarbeiter eigene private Geräte beruflich verwenden oder sollen nur firmeneigene Mobilgeräte genutzt und neu angeschafft werden? Oder beides? Welche Mitarbeiter sollen solch ein Endgerät später überhaupt nutzen?

**Schritt 3: Anbieter wählen**

Hierbei geht es um die Wahl des MDM-Anbieters. Es gibt bereits zahlreiche Hersteller auf dem Markt, wobei die Unterschiede im Angebot oft nur marginal sind. Es sollte ein Anbieter mit Fokus auf die spätere Gesamtlösung gewählt werden. Die spätere MDM-Lösung muss sich nahtlos in diese Infrastruktur einpassen lassen. Unabhängig ob als On-Premise-Lösung oder als Software-as-a-Service-Lösung (SaaS).

**Schritt 4: Die Nutzungsrichtlinie (Policy)**

Die Funktionen einer MDM-Lösung umfassen die Durchsetzung von Nutzungsrichtlinien (Policies) zur Absicherung des Endgeräts inklusive Daten und Apps, Regeln zur Trennung beruflicher und privater Nutzung, der Regulierung des Zugriffs auf interne und externe Daten, Passwortbestimmungen und die externe Steuerung der Geräte für den Notfall.

**Schritt 5: Betriebsrat und Co.**

Neben der technischen Umsetzung sollten organisatorische und rechtliche Gesichtspunkte unbedingt parallel bearbeitet werden. Rechtlich gesehen handelt es sich um Vertragsanpassungen oder Nutzungsvereinbarungen, die Pflichten und Rechte von Arbeitnehmer und -geber, geldwerte Vorteile sowie das Fernmeldegeheimnis abdecken. Auf organisatorischer Seite empfiehlt es sich, den Betriebsrat ebenso wie die Kommunikations- und Personalabteilung frühzeitig in die Planungen mit einzubeziehen, um Datenschutz, Mitarbeiterschutz, Personalschulungen, Nutzerunterstützung (User Support) und begleitende Kommunikationsmaßnahmen aufeinander abzustimmen.

**Schritt 6: Rollout & Pilot**

Ein Pilotprojekt mit einer begrenzten Anzahl von Testnutzern kann bereits im Vorfeld des Rollouts Fehler aufdecken und die Benutzerfreundlichkeit sowie die Umsetzbarkeit der Lösung überprüfen. In dieser Phase können Nachbesserungen vorgenommen, das Nutzerverhalten überwacht und gegebenenfalls durch begleitende Kommunikationsmaßnahmen unterstützt werden.

**Schritt 7: Nutzerunterstützung (User Support) & Beratung**

Bei der Einführung von MDM geht es nicht vorrangig um die reine Technik, sondern um die Mitarbeiter. Diese sollten frühzeitig über die neue Mobility-Strategie des Unternehmens aufgeklärt werden und während als auch nach dem eigentlichen Rollout umfassend geschult und beraten werden. Manche Mitarbeiter müssen sich unter Umständen erst an die neuen Geräte und deren Handhabung gewöhnen. Für ein erfolgreiches MDM ist es wichtig, dass die Mitarbeiter über die technische Bedienung ebenso aufgeklärt werden wie über ihre Rechte und Möglichkeiten.

# 2 Über COMPAREX

## 2.1 Unternehmensvorstellung

COMPAREX ist ein weltweit agierender IT-Dienstleister, der auf Software-Beschaffung, Lizenzierung, Compliance Services, Professional Services sowie technische Produktberatung spezialisiert ist.

Mit seiner mehr als 20-jährigen Markterfahrung adressiert COMPAREX öffentliche Verwaltungen und Mittelstand ebenso wie Industrieunternehmen und international agierende Konzerne. Das Angebotsportfolio umfasst Software-Lizenzen von mehr als 3.000 Herstellern, Beratungs- und Service-Leistungen sowie die projektbezogene Beschaffung von Hardware renommierter Hersteller.

Neben der Expertise für Beschaffung, Management und Lizenzierung von Software bietet COMPAREX umfangreiche, herstellerübergreifende Professional Services an. Zertifizierte und projekterfahrene IT-Spezialisten leisten Beratung, Einführungsunterstützung, Managed Services und Support. Zertifizierte Trainer mit Praxis- und Projekterfahrung schulen Anwender und Administratoren in maßgeschneiderten Seminaren.

Ein besonderer Fokus von COMPAREX Deutschland liegt auf der Entwicklung innovativer und maßgeschneiderter Cloud-Computing-Lösungen.

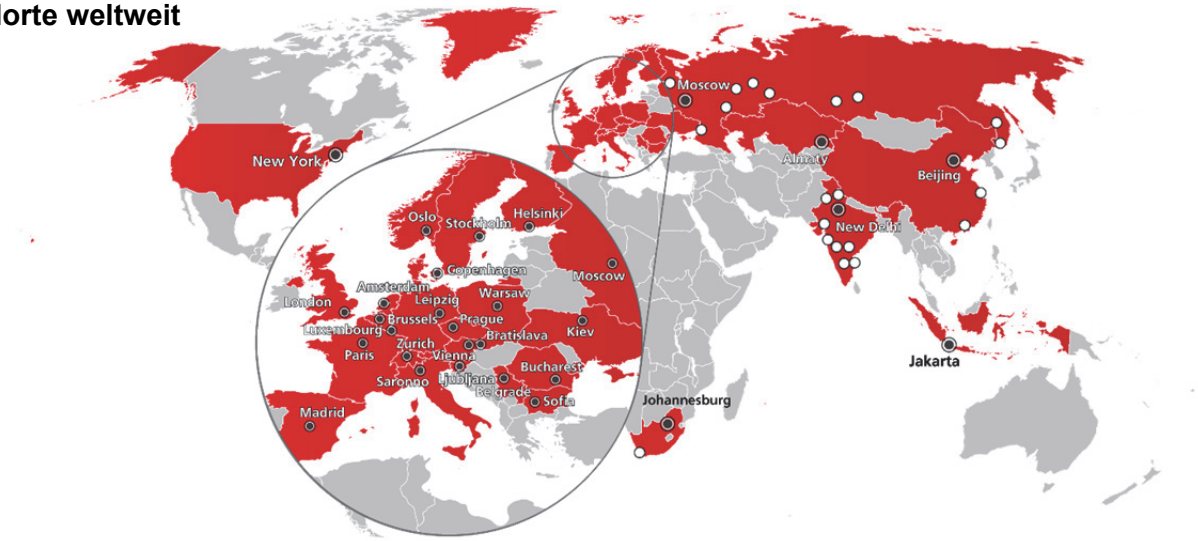
Weltweit beschäftigt die COMPAREX Gruppe rund 1.800 Mitarbeiter an mehr als 75 Standorten in 29 Ländern in Europa, Asien, Afrika und Amerika. Der Umsatz im Geschäftsjahr 2012/13 betrug 1,2 Milliarden Euro.

**COMPAREX Portfolio im Überblick**


Weitere Informationen erhalten Sie unter www.comparex.de.

## 2.2 Standorte

**Standorte weltweit**




**Standorte deutschlandweit**

In Deutschland bedient COMPAREX seine Kunden am Markt mit rund 700 Mitarbeitern in 11 Niederlassungen:


- COMPAREX Leipzig (Hauptsitz)
- COMPAREX Bad Homburg
- COMPAREX Berlin
- COMPAREX Erfurt
- COMPAREX Hamburg
- COMPAREX Hannover
- COMPAREX Köln
- COMPAREX Magdeburg
- COMPAREX München
- COMPAREX Ratingen
- COMPAREX Stuttgart

Um das Wachstum weiter voranzutreiben, hat sich COMPAREX mit einem starken strategischen Investor verbunden – der österreichischen Raiffeisen Group. COMPAREX ist eine 100%ige Tochter der Raiffeisen Informatik GmbH, die eine der führenden Unternehmensgruppen Österreichs mit einer Vielzahl an Beteiligungen international agierender Unternehmen ist.

# 3 Inhalte der Mobile Device Management Nutzungsrichtlinie

## 3.1 Nutzungsberechtigung

- Welche Kollegen haben die Berechtigung für den mobilen Zugriff auf Firmendaten und Firmenapplikationen?
- Wollen Sie zukünftig den Zugriff in Abhängigkeit von individueller Verantwortung einschränken?
  - Rolle
  - Titel
  - Freigabe durch PV
  - Ort des Zugriffes
  - Zugehörigkeit einer Organisationseinheit
  - Andere organisatorische Voraussetzungen

Wenn ja, welche Apps und welche Daten?

- Sollen zukünftig alle privaten Endgeräte (BYOD) unterstützt werden oder gibt es definierte Firmen-Endgeräte? Sollen auch hier Einschränkungen beim Zugriff gemacht werden?

## 3.2 Aufbewahrung und Sicherung

- Sollen Daten und Aktionen der Mobile Devices gesichert und aufbewahrt werden?
- Wer macht das / ist dafür verantwortlich?

Falls ja,

- welche Services (z.B. Anrufliste, Daten, Wi-Fi-Nutzung, Adressen und Kontakte usw.) sollen gesichert und aufbewahrt werden?
- gibt es Dienste die nicht gesichert und aufbewahrt werden (z.B. SMS / MMS, Klingeltöne usw.)?
- sollen kapazitive Obergrenzen und Sicherungszeiträume bei der Aufbewahrung und Sicherung eingeführt werden (z.B. wann wird gesichert, maximale Volumen und maximale Kostenobergrenze usw.)?

## 3.3 Sicherheitsfragen

- Was soll passieren, wenn Endgeräte verloren gehen oder gestohlen werden?
- Was soll passieren, wenn Endgeräte außer Betrieb genommen werden (z.B. Endgeräte-Austausch, Wechsel der Rolle / Verantwortlichkeiten, Nutzer verlässt die Firma usw.)?
  - Löscht das Unternehmen auf dem Endgerät die unternehmensbezogenen Daten oder die Apps oder beides?
  - Darf der Nutzer das Löschen auf dem Endgeräte selbst anstoßen (Self-Service-Portal)?
- Wird ein Passwort (privat und geschäftlich) für die Verwendung des Endgeräts vergeben?
- Dürfen sämtliche Daten / Inhalte auf dem Endgerät gelöscht werden?
- Soll das Firmenpasswort nur für den Firmenteil des Endgerätes gelten („Good Client“)?
- Sollen nur Daten aus dem „Good Client“ gelöscht werden?
- Sollen Einschränkungen für die grundsätzliche Verwendung von Kameras, Browsern, Bluetooth, Applikationen und Services gemacht werden?
- Dürfen User zusätzliche Applikationen im „Good Client“ installieren?
- Was geschieht mit dem Endgerät im Falle einer Infektion mit Malware?

*Vorschläge aus der Praxis:*

Die Nutzungsrichtlinie sollte das „Jailbreaking“ oder andere ähnliche Modifikationen des entsprechenden Endgeräts definitiv verhindern. Es sollten grundsätzlich alle Änderungen, die vom Hersteller-Standard abweichen, untersagt werden. Änderungen des Endgeräts können unternehmensintern als „interner Angriff“ gewertet und entsprechend sanktioniert werden.

Die Nutzungsrichtlinie sollte klare Regulierungen treffen, innerhalb welcher Frist ein verlegtes oder gestohlenes Endgerät bei der IT zu melden ist. Weiterhin sollte klar geregelt sein, ab welcher Frist ein Endgerät im Falle eines Mitarbeiteraustrittes gelöscht wird. Legen Sie die Passwortlänge, die Passwortsicherheit und die Frequenz des Passwortwechsels fest. Beschreiben Sie, wann das Endgerät teilweise oder komplett gelöscht wird.

Legen Sie fest, dass das Unternehmen sich zu jedem Zeitpunkt das Recht der Löschung des Endgerätes vorbehält.

## 3.4 Zulässige Verwendung

- Dürfen andere Personen als der registrierte Nutzer das Endgerät verwenden?
- Darf der Endgeräte-eigene Intranet-Zugang genutzt werden?
  - Wer regelt in diesem Fall die Richtlinien (z.B. Nutzung nicht angemessener Seiten)?

- Wie und wo wird das VPN aufgebaut?

## 3.5 Endnutzer-Support

- Wer bietet dem Endnutzer Unterstützung (Support) an und wo?
- Was wird unterstützt und was nicht?

## 3.6 Verletzungen der Nutzungsrichtlinie (Policy violations)

- Was passiert, wenn ein Nutzer gegen die Nutzungsrichtlinie verstößt?
- Werden unterschiedliche Verstöße unterschiedlich behandelt?