Nutzungshinweise für den Android@DT Service

1 Einleitung

Im Rahmen des Android@DT Service steht Ihnen das Abrufen von PIM-Informationen mit Ihrem Android-Gerät zur Verfügung. Bitte beachten Sie im Rahmen des Service die folgenden Hinweise.

2 Service und Support

- Es wird keine VPN-Verbindung eingerichtet – dadurch ist kein Intranet-Zugriff möglich.
- Es werden nur Postfächer unterstützt, die auf der OS FMO Exchange-Plattform liegen. Dies können Sie durch aufrufen der Outlook Kontoeinstellungen (Outlook → Extras → Kontoeinstellungen → Microsoft Exchange Server) überprüfen. Wenn der Microsoft Exchange-Server mit den Buchstaben „HE“ beginnt, ist Ihr Postfach auf der korrekten Plattform.
- Nur nationale (Deutschland) Anwender mit deutscher Handynummer können am Service teilnehmen.
- PIM-Daten (Email, Kalender, Kontakte, Aufgaben) werden nur mit der App Nitrodesk Touchdown bereitgestellt. Nur zertifizierte Android-Geräte werden für den Service unterstützt.
  Einen Link auf die zertifizierten Endgeräte und Android Versionen finden Sie in der Produktbeschreibung Ihres myMDS oder myTSI - Katalogs.
- Externe SD-Karten werden nicht unterstützt und müssen aus dem Gerät entfernt werden.
- Zur Nutzung des Dienstes ist ein Google-Account erforderlich. Bitte beachten Sie dazu die speziellen Datenschutzhinweise zum Google-Konto (siehe Kapitel 4).
- Die Apps Nitrodesk Touchdown, Sybase Afaria, McAfee, NoTelURL (für Android Version 4.1X) und MoWS PreInstaller werden in einer definierten Version zentral durch das Mobile Device Management zur Verfügung gestellt. Die Aktualisierung, dieser Apps durch Versionen die ggf. im Google Play-Store zur Verfügung stehen, ist nicht gestattet.
- Beachten Sie bitte generell die Hinweise in der Installationsanleitung.

3 Generelle Sicherheitshinweise

3.1 Der Verlust des Endgeräts muss unverzüglich gemeldet werden

Es kann nicht ausgeschlossen werden, dass trotz Geräteverschlüsselung die in den Geräten gespeicherten Zugangskennwörter zu der Infrastruktur der DTAG extrahiert werden, daher müssen diese Passwörter zeitnah geändert werden, wenn das Gerät verloren / gestohlen wird. Der Benutzer hat einen Verlusts unverzüglich, sofern möglich binnen einer Stunde, spätestens jedoch am Morgen des nächsten Werktags an den Help Desk unter der Rufnummer: 0800 4967538 zu melden.
Diebstähle müssen an das GBS-Casemanagement (GBS-Casemanagement@telekom.de) gemeldet werden.

3.2 Kein Anschluss/Synchronisation der Endgeräte an nicht durch die DT gemangten PCs

Da bei einem Anschluss an einen nicht gemanagten PC (zum Beispiel privat PC) mit der Hersteller-Software automatisch ein Backup der auf dem Android-Gerät befindlichen Unternehmensdaten auf dem

nicht gemanagten PC angestoßen werden kann, ist die Verbindung/ Synchronisation mit einem nicht gemanagten PC nicht gestattet.

Ausgenommen von diesem Verbot sind ausschließlich die nachstehenden 2 Fälle, bei denen der Mitarbeiter das Android-Gerät mit einem nicht gemanagten PC sofern zutreffend verbinden darf:

1. Die Aktivierung des Endgerätes beim Hersteller zur Inbetriebnahme des Android-Geräts.
2. Die Aktualisierung auf eine durch DTAG freigegebene Firmware/ Softwarepatch.
   Hierbei hat der Mitarbeiter sicherzustellen, dass vor Verbinden eines Android-Geräts mit dem nicht gemanagten PC ein lokaler Wipe (löschen aller auf dem Android-Geräts befindlichen Unternehmensdaten) erfolgreich ausgeführt wurde.

Sollte es im Einzelfall dennoch zu einem versehentlichen Anschluss an einen nicht gemanagten PC kommen, muss das angefertigte Backup unverzüglich und sicher durch den Benutzer gelöscht werden.

Diese Regelung gilt sowohl für die leitungsgebundene Synchronisierung als auch für die Synchronisierung per Funkschnittstelle.

3.3 Keine Verwendung von Jailbreaks/Root-Rechte

Durch die Verwendung von sogenannter Jailbreak/Root-Rechte Software (z.B. zur Überwindung von werkseitig implementierten Sicherheitsmechanismen) wird die Sicherheit des gesamten Systems unterlaufen. Aus diesem Grunde ist die Verwendung von Jailbreaks/Root-Rechten nicht zulässig.

3.4 Update der Firmware auf dem Android-Device

Der Mitarbeiter ist verpflichtet, selbständig Updates des Betriebssystems zeitnah nach Freigabe durchzuführen.
Die Nutzung einer nicht freigegebenen Firmware-Version kann zu technischen Problemen und zum Ausschluss aus dem Service führen. Automatische OTA(Over The Air) -Updates sind in den Benutzereinstellungen zu deaktivieren.
Einen Link auf die zertifizierten Endgeräte und Firmware-Versionen finden Sie in der Produktbeschreibung Ihres myMDS oder myTSI - Katalogs.

3.5 Installation von Applikationen (Apps)

Bei der Installation von Applikationen (Apps) ist mit besonderer Sorgfalt darauf zu achten, aus welcher Quelle bzw. von welchem Hersteller die Applikation stammt. Grundsätzlich dürfen nur Apps aus vertrauenswürdigen Quellen bzw. von vertrauenswürdigen Herstellern installiert werden.

Bitte informieren Sie sich bzgl. der Sicherheitsbewertung der gewünschten App deshalb unbedingt vorher noch an einer anderen Stelle als im Google Playstore.
Während des Installationsvorgangs sollten die von der Applikation angeforderten Rechte genau geprüft und im Zweifel die Installation abgebrochen werden. Des weiteren sollten während der Installation unbedingt auch die Meldungen des Virenscanners beachtet werden.

3.6 Keine Beschaffung von Applikationen (Apps) auf Rechnung des Arbeitgebers

Es ist dem Mitarbeiter untersagt, kostenpflichtige Applikationen (Apps) aus einem auf dem mobilen Gerät angebotenen AppStore/Market auf Rechnung des Arbeitgebers herunterzuladen und zu installieren. Dies gilt insbesondere für den Service der Abrechnung von Einkäufen über die Mobilfunkrechnung.

3.7 eMail-Signatur

Das Unternehmen unterliegt bestimmten Kennzeichnungspflichten für ausgehende Korrespondenz. Aus diesem Grund hat der Mitarbeiter dafür Sorge zu tragen, dass bei ausgehenden Nachrichten die korrekte eMail-Signatur verwendet wird.
Bei einer Änderung ist der Mitarbeiter verpflichtet, die Signatur eigenverantwortlich anzupassen.

3.8 Passwörter interner Applikationen und Passwörter generell

Die Klartextspeicherung von Kennwörtern auf dem mobilen Endgerät ist nicht erlaubt (z.B. Notizen-App).

Der Android Standard-Browser speichert alle Passwörter im Klartext. Die Verwendung von Passwörtern im Browser ist daher zu unterlassen.

Eine Besonderheit tritt bei Samsung Geräten auf. Die Samsung Tastatur speichert in der Standard-Einstellung auch Passwörter. Diese werden als „Auto-Suggestion“ beim Tippen von Texten vorgeschlagen. Um zu verhindern, dass Dritte so Kenntnis von Passwörtern erlangen können, ist die Eingabehilfe entsprechend so zu konfigurieren, dass die „Autovervollständigung“ deaktiviert wird. Das kann unter „Einstellungen/Sprache und Eingabe/erweiterte Einstellungen durchgeführt werden.

3.9 Nutzung von Kontaktdaten

Bitte beachten Sie, dass Kontaktdaten im Android/Touchdown Adressbuch nur zu geschäftlichen Zwecken verwendet werden dürfen. Eine Synchronisation/Weitergabe dieser Kontaktdaten mit Apps, Webseiten, Portalen, anderen Email-Konten oder ähnlichem darf nicht erfolgen.
Kontakte dürfen nur von Touchdown mit dem geschäftlichen Email-Adressbuch synchronisiert werden. Der Zugriff auf die geschäftlichen Kontaktdaten über eine Drittanwendung (z.B. 3rd-Party Apps) ist nicht erlaubt.
Sollten Sie beobachten, dass Kontakte ungewollt durch 3rd-Party Apps o.ä. synchronisiert werden, informieren Sie bitte umgehend den Help Desk unter der Rufnummer: 0800 4967538.

3.10 Public Cloud Services

Die Nutzung von Public Cloud Services als auch von Fernzugriffdiensten wie z.B. Samsung Dive ist nicht gestattet.

4 Datenschutz-Hinweise zu Google- bzw. Hersteller-Konten bei Android@DT Services

Was ist zu tun?

Für die Nutzung eines Endgeräts mit dem Betriebssystem Google ANDROID in Verbindung mit den Mobile Workplace Services (MoWS) benötigen Sie zwingend ein Benutzerkonto bei Google (nachfolgend „Google-Konto“ genannt).
In den meisten Fällen wird dieses Konto bereits bei der Einrichtung des Endgerätes abgefragt oder eingerichtet.

Um eine Trennung von dienstlicher und privater Nutzung zu ermöglichen, verwenden Sie auf einem **dienstlich genutzten Gerät NICHT Ihr möglicherweise existierendes, privates Google-Konto**! Nehmen Sie sich die Zeit, und erstellen Sie sich ein separates Google-Konto für dienstliche Nutzung. Umgekehrt dürfen Sie dieses dienstliche Google-Konto nicht für private Zwecke benutzen.

Zur dienstlichen E-Mail Kommunikation achten Sie darauf, **ausschließlich** die für diesen Zweck installierte Applikation „**NitroDesk TouchDown**“ zu **benutzen**. Eine Nutzung von z.B. Google Mail für dienstliche Zwecke ist nicht erlaubt.

Um eine versehentliche Nutzung auszuschließen, **deaktivieren** Sie gemäß der Bedienungsanleitung zu MoWS **die Synchronisierung von E-Mail, Kalender und Kontakten Ihres Geräts mit dem Google Konto**.

Um vor akuten Gefahren durch Schwachstellen und Schadsoftware geschützt zu sein, halten Sie die Software Ihres Geräts durch entsprechende Updates auf dem aktuellen Stand und installieren Sie nur Software, die dienstlich erforderlich ist. Sie verpflichten sich mit der dienstlichen Nutzung, nach bestem Wissen nur Updates und vertrauenswürdige Software auf das Gerät zu laden.

Haben Sie den Verdacht oder sind Sie sich sicher, dass doch einmal vertrauliche Daten in die falschen Hände geraten sind, informieren Sie den Datenschutz unter folgender Mailadresse: Datenschutz@telekom.de

Die Datenschutzbestimmungen von Google sind öffentlich einsehbar unter http://www.google.com/intl/de/policies/privacy/.

Was kann passieren?

Über das Google-Konto können alle hiermit verbundenen Aktivitäten und Daten mit dem Kontoinhaber (also Ihnen) in Verbindung gebracht werden. Beispielsweise kennt Google durch die Verknüpfung des Kontos mit Ihrem Endgerät alle installierten Programme. Wenn Sie Dienste, wie z.B. Google Latitude oder Google Places nutzen, kennt Google zudem Ihren Standort und könnte somit Bewegungsprofile erstellen.

Im Sinne der Selbstauskunft stellt Google die verknüpften Daten im sogenannten „Dashboard“ (https://www.google.com/dashboard/) zusammen – hierüber können Sie die bei Google mit Ihrem Konto verbundenen Daten einsehen.

Welche Daten werden erhoben?

Google fragt für die Erstellung des Google-Kontos Ihren Vor- und Nachnamen, sowie Ihre E-Mail Adresse ab. Weiterhin vergeben Sie sich bei der Kontoerstellung einen frei wählbaren Namen mit der Endung @gmail.com.

MoWS selbst verarbeitet neben Ihrem Namen und der dienstlichen E-Mail Adresse die zur Geräteverwaltung benötigten Daten rund um Ihr Endgerät (Rufnummer, Modell, IMEI, Software-Versionen). Die Daten werden ausschließlich zum Zweck der Diensterbringung erhoben, gespeichert und verarbeitet.

Was ist mit Konten bei Geräte-Herstellern (z.B. HTC, Samsung)?
Ein Hersteller-Konto sollten Sie nur dann anlegen, wenn es zur Aktualisierung der Firmware Ihres Gerätes notwendig ist.

Hiermit bestätige ich, dass ich diese Nutzungshinweise verstanden und vollständig zur Kenntnis genommen habe.