



Republik Österreich

**Datenschutz
behörde**

A-1080 Wien, Wickenburggasse 8

Tel.: +43-1-52152-2569

E-Mail: dsb@dsb.gv.at

DVR: 0000027

**Angaben zur Datenanwendung
Meldung einer Datenanwendung (gemäß Anlage 2 DVRV 2002BGBl. II Nr. 24/2002)**

Art der Meldung:

- Neumeldung einer Datenanwendung
- Änderung einer Datenanwendung

Bezeichnung der Datenanwendung und Zweck der Datenanwendung

Mobile Device Management Software (MDM; konkret "MobileIron") zur sicheren Konfiguration, Verwaltung und Überwachung der Compliance von mobilen Endgeräten - Android Smartphones und Tablets sowie iPhones und iPads - die den MitarbeiterInnen zur Verfügung gestellt werden und im Eigentum der Auftraggeberin stehen. Über die MDM-Software erhalten die MitarbeiterInnen im Haus Graz standardmäßig Zugriff auf Outlook Exchange und das Haus-Graz-interne WLAN auf den mobilen Geräten. Die Bereitstellung weiterer Services und Apps über die MDM-Software ist möglich.

Registernummer:

0051853

Nummer der Datenanwendung

0051853/408

Name (sonstige Bezeichnung) und Anschrift des Auftraggebers:

Magistrat der Stadt Graz
Hauptplatz 1
8011 Graz
Österreich

Telefon- und Faxnummer sowie E-Mail-Adresse des Auftraggebers:

Tel.: 0316 872 2336
walther.nauta@stadt.graz.at

Vertreter des Auftraggebers:

Vertreter des Auftraggebers in der EU bei der Datenanwendung:

Datenschutzbeauftragter:

Die Datenanwendung gehört zum

- privaten Bereich
 öffentlichen Bereich

Die Datenanwendung erfolgt

- automationsunterstützt
 manuell

Angaben zur Anwendbarkeit der Vorabkontrolle (§ 18 Abs. 2 DSG 2000):

- Verwendung von sensiblen Daten
 Verwendung von strafrechtlich relevanten Daten
 Vorliegen eines Kreditinformationssystems
 Vorliegen eines Informationsverbundsystems
 Videoüberwachung (gemäß § 50c DSG 2000)
 Vorliegen keiner der Voraussetzungen

Rechtsgrundlage(n) für die gemeldete Datenanwendung

§ 8 Abs 1 Z 2 und Z 4 DSG 2000; IT-Sicherheitsrichtlinien für die Stadt Graz; Servicevereinbarungen zwischen der Stadt Graz und der ITG Informationstechnik Graz GmbH

Bescheid der Datenschutzbehörde (Internationaler Datenverkehr gemäß § 13 DSG 2000):**Bescheid der Datenschutzbehörde (Auflagenbescheid gemäß § 21 Abs. 2 DSG 2000):****Besondere Angaben zum Inhalt der Datenanwendung:**

Betroffene Personengruppen	Datenarten	Nummern der Empfängerkreise
Bedienstete der Stadt Graz, denen ein mobiles Endgerät zur Verfügung gestellt wird	Name (Vorname, Nachname)	
	Organisations-/Abteilungszugehörigkeit	
	Userdaten (LDAP-Referenz (LDAP-Username und Organisationszugehörigkeit, Gruppenzugehörigkeit), macOS User ID und Name)	
	Telefonnummer	
	E-Mail-Adresse	
	IP-Adresse	
	Geräteerkennung (Geräte-UUID, IMEI, ICCID, IMSI, UDID, WP Publisher Device ID)	
	Hardware (Hersteller, Hardware Version, MAC-Adresse, Firmware-Version, Prozessortyp/-architektur, Display-Größe)	
	Betriebssystem (OS Version, OS Update Status)	
	Gerätestatus/-konfiguration (Akkustand, Background-Status, Standorteinstellungen, Status Standorterkennung,	

	Speicherplatz/verfügbarer Speicher, Hotspot-Status, Roaming-Status, Geräte- und -eigentümer, Sprach- und Ländereinstellung und weitere Konfigurationsdaten)	
	Netzbetreiberinformationen (Netzwerkcode, Betreibername, Mobilfunktechnologie, Länderkennung)	
	Push-Notification-Funktionalität (Status, Token)	
	PIN/Passwort für Sperrbildschirm und Löschmöglichkeit samt Status	
	MDM (MobileIron) -Client (ID, Version, Name, Build Datum)	
	Informationen zum Mobile Iron Container (Liste der installierten Apps, Datum der Installation/Deinstallation)	
	Liste aller installierten Apps (keine Inhaltsdaten)	
	Informationen zum MDM-Client (Build Date, Last Check-In, Name, Version)	
	MDM-Status (Status Lost Mode, letztes MDM-Portal Login, letzte Kommunikation mit MDM-Server, Tunnel App Status, Multi MDM)	
	Daten bzgl. Sicherheitskonfiguration/-zustand des Gerätes (Antivirus-Status, Signature-Status, Data-Execution-Prevention-Policy, Reset/Restart Count, Safe Mode, Datum des letzten Hotfix und weitere Konfigurationsdaten)	
	Compliance-Status und Datum; Quarantäne-/Sperr-Status und Begründung	
	Verschlüsselung (Status Disk/SD Card, Secure Apps Encryption, Bitlocker Passwort/Pin)	
	Backup-Status	
	Exchange (letzte Sync-Zeit und Exchange ID)	
	letzter Standort des Gerätes (Abfrage im Verlustfall bei entsprechender Einwilligung des Betroffenen)	
Administratoren der MDM-Software	Name (Vorname, Nachname)	
	Zuordnung ActiveDirectory-Account (ActiveDirectory-	

	Username)	
	Berechtigungen	
	Log über vorgenommene Konfigurationen/Einstellungen	
	Allgemeine Kommentare zum MDM eines Gerätes	

Beabsichtigte Übermittlungen aus dieser Datenanwendung:

Nummer und Bezeichnung des Empfängerkreises	Rechtsgrundlage für die Übermittlung
--	---