Datenschutz bei App-Nutzung auf unternehmenseigenen Smartphones und Tablets

Zusammenfassung: Nutzen Beschäftigte vorinstallierte Apps auf unternehmenseigenen Smartphones und Tablets, so haftet das Unternehmen als Eigentümer des Smartphones bzw. Tablets für Datenschutzverletzungen, die eintreten können, wenn die durch das Unternehmen vorinstallierten Apps personenbezogene Daten der Beschäftigten an die App-Betreiber weiterleiten. Daran ändert in der Regel auch ein MDM (mobile device management) nichts, es sei denn, es ist so konfiguriert, dass der unkontrollierte Datenabfluss ausgeschlossen ist und die restriktiven Einstellungen auch nach Betreiber-Updates nicht verändert werden.

Der Praxisfall aus der Sicht eines Unternehmers: Meinen Mitarbeitern stelle ich ein Smartphone des Unternehmens zur Verfügung. Darauf sind bestimmte Apps installiert. Die ABGs dieser Apps sind oft auf Englisch abgefasst, im Übrigen so kompliziert, dass man den Eindruck hat, nur noch Juristen verstehen das, selbst wenn die AGBs auf Deutsch sind. Wer haftet, wenn nun Personendaten wie Standort, Bewegungsprofile usw. über meine Beschäftigten, deren Persönlichkeitsrechte dadurch verletzt werden können, an die App-Betreiber übermittelt werden?

Situation: Viele Unternehmen erkennen die Möglichkeiten zur Produktivitätssteigerung und stellen ihren Beschäftigten unternehmenseigener Smartphones und Tablets zur Verfügung. Wenn das Unternehmen der Eigentümer der Geräte ist, haftet die Geschäftsführung grundsätzlich auch für den Abfluss personenbezogener Daten an die App-Betreiber. Die Betriebssysteme sind in der Regel so eingestellt, dass bei Installation einer neuen App eine dezidierte Zustimmung zur Weitergabe der dort aufgeführten personenbezogenen Daten erteilt werden muss. Dabei werden vor der Installation der App Berechtigungen eingefordert, die hinsichtlich Datenschutzes sehr genau geprüft werden müssen.

Rechtslage: Wenn von unternehmenseigenen Geräten personenbezogene Daten von Beschäftigten an Dritte übermittelt werden sollen, muss dafür ein Ausnahmetatbestand gemäß § 4 Abs. 1 BDSG vorliegen. Da hier als Ausnahmetatbestände eine Regelung im Bundesdatenschutzgesetz (oder einem anderen relevanten Datenschutzgesetz wie das jeweilige Landesdatenschutzgesetz, eines der kirchlichen Datenschutzgesetzte oder eine andere gegebenenfalls einschlägige rechtliche Regelung) vorliegen muss, ist zu prüfen, ob dies gegeben ist. Ansonsten liegt mit großer Wahrscheinlichkeit eine unerlaubte Übermittlung personenbezogener Daten an Dritte vor.

Bei App-Betreibern erfolgt oft eine Übermittlung in Drittländer: Erschwerend kommt hier hinzu, dass viele der App-Betreiber ihren Sitz nicht in einem EU-Land oder einem Land des erweiterten Wirtschaftsraumes haben, sondern in einem potenziell unsicheren Drittland, wie das beispielsweise bei WhatsApp der Fall ist. Hier für die datenschutzkonforme Nutzung einer App eine rechtssichere Vereinbarung herzustellen, dürfte in der Praxis ein schwieriges, nahezu unmögliches Unterfangen sein.

Wem gehören die Daten? Die personenbezogenen Daten gehören dem Beschäftigten selbst. Werden diese über ein Gerät, das der Arbeitgeber zur geschäftlichen Nutzung überlassen hat, unbefugt an Dritte übermittelt, haftet grundsätzlich der Arbeitgeber für diesen Tatbestand. Ohne ein dezidiertes Einverständnis der Beschäftigten in die Datenübermittlung ist das Risiko einen Verstoß gegen geltendes Datenschutzrecht zu begehen eigentlich nicht zu umgehen. Diese Einverständniserklärung muss dann den Anforderungen des § 4a BDSG entsprechen.

Updates beachten! Da mit der Auslieferung von Updates sich die Datenanforderungen der App-Hersteller verändern können, muss diese Tatsache berücksichtigt werden. Allerdings ist es mehr als zweifelhaft, ob eine Einverständniserklärung eines Beschäftigten rechtsgültig für mögliche Updates eingeholt werden kann, so dass hier ein nicht kalkulierbares Risiko bleibt.

Handlungsempfehlung: Apps ohne Ende-zu-Ende-Verschlüsselung und ohne Garantie, EU-Datenschutznormen einzuhalten, haben auf unternehmenseigenen Smartphones und Tablets nichts verloren. Vor der Ausgabe eines Smartphones oder Tablets an Beschäftigte zur betrieblichen Nutzung sollte sehr genau geprüft werden, welche Datenanforderungen die Apps haben, um genutzt werden zu können. Bei Updates sollte im Einzelfall geprüft werden, ob die zuvor sicheren Datenschutzeinstellungen noch sicher sind.

Eberhard Häcker, Ensdorf