Sachstand

Risiken bei der Nutzung privater Endgeräte für den dienstlichen Bereich

Risiken bei der Nutzung privater Endgeräte für den dienstlichen Bereich

Aktenzeichen:	WD 7 - 3000 – 059/19
Abschluss der Arbeit:	27.03.2019
Fachbereich:	WD 7: WD 7: Zivil-, Straf- und Verfahrensrecht, Umweltschutzrecht, Bau und Stadtentwicklung

Inhaltsverzeichnis

1. Einleitung

Die Nutzung privater Endgeräte für den dienstlichen Gebrauch, häufig als „Bring Your Own Device“ bezeichnet, bietet zahlreiche juristische Risiken. Der Arbeitnehmer speichert betriebsinterne Daten auf seinem Endgerät und kommuniziert dienstlich mit Kunden und anderen unternehmensinternen Mitarbeitern. Dabei können den Beschäftigten unter anderem bestimmte Dokumentations- und Aufbewahrungspflichten treffen. Auch besteht ein gewisses Haftungsrisiko für den Arbeitnehmer.

2. Dokumentations- und Aufbewahrungspflichten

Mit der Einbeziehung privat angeschaffter Geräte in die unternehmenseigene IT-Struktur können diese den handels- oder steuerrechtlichen Dokumentations- und Archivierungspflichten unterliegen.

§ 257 Abs. 1 HGB[1] verpflichtet jeden Kaufmann, bestimmte in seinem Geschäftsbetrieb anfallende Unterlagen geordnet für einen Zeitraum von 6 Jahren oder im Falle von Buchungsbelegen sogar für 10 Jahre aufzubewahren. Darunter können auch Messenger-Nachrichten fallen, wenn sie empfangene oder abgesandte Handelsbriefe oder Buchungsbelege enthalten. Handelsbriefe sind Schriftstücke, die ein Handelsgeschäft i.S.d. §§ 343, 344 HGB betreffen. Dazu zählen alle Schriftstücke, die der Vorbereitung, dem Abschluss, der Durchführung oder Rückgängigmachung von Handelsgeschäften dienen, wie etwa Angebote, Bestellungen oder Rechnungen. Aufbewahrungspflichtig sind, auch im Wege der Datenfernübertragung (EDI, E-Mail, Internet usw.) übersendete Nachrichten. Ein bestimmtes Aufbewahrungsformat wird diesbezüglich nicht vorgeschrieben.[2]

Die meisten Messenger-Dienste speichern die Chat-Nachrichten, die vom jeweiligen Kommunikationspartner abgerufen und gelesen wurden nicht, sodass zur Erfüllung der beschriebenen handelsrechtlichen Aufbewahrungspflichten regelmäßig nicht auf den Betreiber des Messenger-Dienstes und dessen zentrale Infrastruktur zurückgegriffen werden kann. Die Chat-Nachrichten werden nur in den Smartphones der Kommunikationspartner gespeichert. Allerdings besteht die Möglichkeit, Chat-Verläufe zu exportieren und sie z.B. in einem Cloud-Speicher abzulegen oder sich per E-Mail zuzusenden. Ferner existieren entgeltpflichtige Tools, die den Export der Chatverläufe samt Anhängen auf einen PC mit lesbarer Darstellung als HTML, PDF, Doc oder CSV-Files ermöglichen.[3]

---

1 Handelsgesetzbuch, vom 10.05.1897 (RGBl. S. 219), zuletzt geändert durch Art. 3 G zur Ausübung von Optionen der EU-ProspektVO und zur Anpassung weiterer Finanzmarktgesetze vom 10.07.2018 (BGBl. I S. 1102).

2 Böcking/Gros, in: Ebenroth/Boujong/Joost/Strohn, Handelsgesetzbuch, 3. Auflage 2014, § 257 HGB, Rn. 9.

3 Schrey/Kielkowski/Gola: Chatten für den Arbeitgeber, MMR 2017, S. 656 ff. (659).

Die steuerrechtlichen Aufbewahrungs- und Dokumentationspflichten in § 147 Abs. 1 AO[4] entsprechen den handelsrechtlichen Aufbewahrungspflichten und ergeben daher keine weiteren Verpflichtungen für Unternehmen. Allerdings hat gem. § 147 Abs. 6 S. 1 AO die Finanzbehörde im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen, wenn diese Unterlagen mithilfe „eines Datenverarbeitungssystems“ erstellt wurden. Verblieben die als Handelsbriefe zu qualifizierenden Messenger-Nachrichten zwischen Unternehmensmitarbeitern und Kunden lediglich auf den Smartphones der Mitarbeiter und würden nicht zentral bei dem Unternehmen gespeichert werden, könnte dieses seinen Verpflichtungen aus § 147 Abs. 6 AO gegenüber der Finanzbehörde nur schwer nachkommen.[5]

Bei der Ausgestaltung eines Konzepts für „Bring Your Own Device“ ist auf die Dokumentations- und Aufbewahrungspflichten insofern besondere Rücksicht zu nehmen.[6] Um dies zu gewährleisten kann das Unternehmen die betriebliche Partition des Smartphones regelmäßig mit den Servern des Unternehmens synchronisieren und den Arbeitnehmer zusätzlich zur regelmäßigen Vornahme einer manuellen Datensicherung anweisen oder verpflichten.[7]

3. Strafrechtliche Aspekte

Speichert der Arbeitnehmer sensible, betriebsinterne Daten auf seinem mobilen Endgerät und überlässt er dieses Dritten (beispielsweise Familienangehörigen oder Freunden), so kann eine Strafbarkeit wegen Verrats von Betriebs- und Geschäftsgeheimnissen nach §§ 17, 18 UWG[8] in Betracht kommen.[9] Geschäfts- oder Betriebsgeheimnis ist jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten Willen des Betriebsinhabers, der auf einem ausreichenden wirtschaftlichen Interesse beruht, geheim gehalten werden soll.[10] Haben Familienangehörige des Arbeitsnehmers nur im Rahmen privater Nutzung Zugriff auf das mobile Endgerät des Arbeitnehmers, kommt regelmäßig kein Verstoß gegen §§ 17, 18 UWG in Betracht, soweit eine etwaige Offenbarung an Familienangehörige nicht zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten

---

4 Abgabenordnung (AO), in der Fassung der Bekanntmachung vom 01.10.2002 (BGBl. I S. 3866, ber. 2003 S. 61), zuletzt geändert durch Art. 15 Gesetz zur Umsetzung des Gesetzes zur Einführung des Rechts auf Eheschließung für Personen gleichen Geschlechts vom 18.12.2018 (BGBl. I S. 2639).

5 Schrey/Kielkowski/Gola: Chatten für den Arbeitgeber, MMR 2017, S. 656 ff. (659).

6 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil V. Kapitel 2. Bring Your Own Device und Datenschutz, Rn. 22, 23.

7 Göpfert/Wilke: Nutzung privater Smartphones für dienstliche Zwecke, NZA 2012, S. 765 ff. (768).

8 Gesetz gegen den unlauteren Wettbewerb (UWG), in der Fassung der Bekanntmachung vom 03.03.2010, (BGBl. I S. 254), zuletzt geändert durch Art. 4 G zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts vom 17.02.2016 (BGBl. I S. 233).

9 Kremer/Sander, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Auflage 2018, 4. Nutzungsvereinbarung zu „Bring Your Own Device“ (BYOD), Rn. 15, 16.

10 Ohly, in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Auflage 2016, § 17 UWG, Rn. 5.

eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen geschieht.[11]

In Betracht kommt daneben eine Strafbarkeit des Arbeitnehmers nach § 203 StGB, wenn er Berufsgeheimnisträger im Sinne von § 203 Abs. 1 StGB ist oder der Tätergruppe des § 203 Abs. 2 StGB angehört. Voraussetzung ist aber ebenfalls, dass der Beschäftigte zumindest bedingt vorsätzlich handelt.[12]

***

11 Conrad, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Auflage 2016, § 37, Rn. 311.

12 Conrad, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Auflage 2016, § 37, Rn. 313.