



Sachstand

Nutzung privater Endgeräte für den dienstlichen Gebrauch

Nutzung privater Endgeräte für den dienstlichen Gebrauch

Aktenzeichen: WD 3 - 3000 - 089/19
Abschluss der Arbeit: 10 .05.2019
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

1. Fragestellung

Der Sachstand thematisiert datenschutzrechtliche Aspekte einer dienstlichen Nutzung von privaten Endgeräten, auf denen personenbezogene Daten gespeichert werden. Aufgezeigt wird der allgemeine datenschutzrechtliche Rahmen. Eine abschließende Darstellung kann nicht erfolgen, da diese eine Prüfung des Einzelfalles voraussetzt, die insbesondere die Art der zu speichernden Daten sowie die konkreten Verarbeitungsvorgänge berücksichtigen müsste.

2. Datenschutzrechtliche Verantwortlichkeit

Die datenschutzrechtlichen Vorgaben binden den datenschutzrechtlich **Verantwortlichen**. Bei einer Nutzung privater Endgeräte zu dienstlichen Zwecken ist daher zunächst zu prüfen, wer als Verantwortlicher anzusehen ist. Nach Art. 4 Nr. 7 der Datenschutz-Grundverordnung (DSGVO) ist ein Verantwortlicher „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; [...]“.

Folgt man der dargelegten Legaldefinition ist jedenfalls der **Arbeitgeber** als Verantwortlicher anzusehen. Die Datenverarbeitung erfolgt für den Arbeitgeber. Der Arbeitnehmer ist darüber hinaus wegen seiner arbeitsvertraglichen Pflichten und der Direktionsgewalt des Arbeitgebers nicht frei, über die Art und Weise der Verarbeitung zu entscheiden.¹ Unerheblich ist daher, ob die Datenverarbeitung im räumlichen Herrschaftsbereich des Arbeitgebers erfolgt.²

Auf der Seite des **Arbeitnehmers** dürfte in der Regel die Verantwortlicheneigenschaft fehlen, da die Verarbeitung aufgrund des Abhängigkeitsverhältnisses dem Arbeitgeber zugerechnet wird.³ Etwas anderes kann jedoch im Rahmen echter freier Mitarbeiterverhältnisse gelten, da hier die Datenverarbeitung durch eine rechtlich selbstständige Stelle erfolgt.⁴

Aus datenschutzrechtlicher Sicht problematisch ist auch die Einordnung der personenbezogenen Daten, die vom Arbeitnehmer **privat** auf dem Endgerät **gespeichert** werden. Findet zwischen den Datenbeständen keine technische oder organisatorische Trennung statt,⁵ werden auch die privaten Daten nach Ansicht in der Literatur von der betrieblichen Nutzung infiziert.⁶ Eigentlich

1 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 33; so bereits zum alten Recht: Hoppe, in: Kramer, IT-Arbeitsrecht, 1. Aufl. 2017, Rn. 627.

2 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 34.

3 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 36.

4 Zu diesem Komplex und der Anwendung des Art. 28 DSGVO: Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 36.

5 Vorgeschlagen wird hierzu etwa die Nutzung sog. Container Apps. Vgl. hierzu: Möhren, in: Hümmerich/Lücke/Mauer, Arbeitsrecht 9. Aufl. 2018, § 3 Rn. 206.

6 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 27; Zerdick, in: Ehmman/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 2 Rn. 11.

könnte sich ein Privater bei der Datenspeicherung auf seinen Endgeräten auf Art. 2 Abs. 2 lit. c) DSGVO berufen, wonach die Datenverarbeitung durch natürliche Personen zu ausschließlich persönlichen und familiären Zwecken nicht dem sachlichen Anwendungsbereich der DSGVO unterfällt. Die Ausnahmvorschrift wird jedoch eng ausgelegt.⁷ Eine gemischte und vor allem auch ungetrennte Datenspeicherung führt damit unter Umständen auch zu einer Verantwortlichkeit des Geräteinhabers, jedenfalls im Hinblick auf die von ihm zu privaten Zwecken gespeicherten personenbezogenen Daten.⁸

3. Pflichten des datenschutzrechtlich verantwortlichen Arbeitgebers

Nach Art. 24 Abs. 1 DSGVO hat ein Verantwortlicher durch geeignete **technische und organisatorische Maßnahmen** sicherzustellen, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Bei der Nutzung mobiler Geräte muss auf spezifische Risiken geachtet werden, die sich insbesondere aus einem Zugriff unbefugter Dritter oder bei Verlust des Gerätes ergeben können.⁹ Daneben wird nahezu einhellig gefordert, dass private und betriebliche Daten getrennt voneinander gespeichert werden müssen.¹⁰

In der Literatur wird zudem diskutiert, ob die Nutzung privater Endgeräte als eigenständige Verarbeitungsform eine Pflicht zur Durchführung einer **Datenschutz-Folgenabschätzung** gem. Art. 35 DSGVO nach sich zieht.¹¹

Ferner dürfte auch die **Meldepflicht** des Art. 33 DSGVO an die Aufsichtsbehörde bzw. die im Einzelfall korrespondierende **Benachrichtigungspflicht** nach Art. 34 DSGVO an die betroffene Person greifen. Beide Pflichten greifen im Falle einer Verletzung des Schutzes personenbezogener Daten und dürften vor allem bei einem Geräteverlust zur Anwendung kommen.¹²

4. Kontrollmöglichkeiten des Arbeitgebers und des Datenschutzbeauftragten

Die Kontrollmöglichkeiten des **Arbeitgebers** sind aufgrund des entgegenstehenden Eigentums des Arbeitnehmers an seinen mobilen Geräten beschränkt. Hinzu kommt zudem der Schutz der privat gespeicherten personenbezogenen Daten, der einen Zugriff des Arbeitgebers erschwert. Aus diesem Grunde wird ein originäres Zugriffs- und Kontrollrecht des Arbeitgebers in der Literatur

7 Vgl. EuGH, Urteil vom 11.12.2014 - C-212/13 (Ryneš).

8 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 30.

9 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 40.

10 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 41; Möhren, in: Hümmelich/Lücke/Mauer, Arbeitsrecht 9. Aufl. 2018, § 3 Rn. 206; Brandt, in: Hauschka/Mossmayer/Lösöer, Corporate Compliance, 3. Aufl. 2016, § 29 Rn. 155; Hoppe, in: Kramer, IT-Arbeitsrecht, 1. Aufl. 2017, Rn. 630.

11 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 42.

12 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 71 f.

verneint.¹³ Kontrollmöglichkeiten können daher nur aufgrund einer Regelung im Arbeitsvertrag oder kollektivarbeitsrechtlich eingeräumt werden. Entsprechende Regelungen müssen den Grundsatz der Verhältnismäßigkeit wahren. Zudem beschränkt sich die Kontrolle auf betriebliche Datensätze. Ist hierbei eine Trennung von privaten Daten organisatorisch nicht möglich, müssen entsprechende Kontrollen den Zugriff auch auf privat gespeicherte Datensätze auf das Notwendige beschränken.¹⁴ Die privaten Daten sollten zudem nach Trennung von den betrieblichen Daten arbeitgeberseitig unverzüglich gelöscht werden.

Soweit ein Arbeitgeber der Pflicht zur Bestellung eines **betrieblichen Datenschutzbeauftragten** unterliegt (vgl. Art. 37 DSGVO) erstrecken sich auch dessen Kontrollbefugnisse auf die dienstlich genutzten privaten Endgeräte. Hierbei gelten ähnliche Maßstäbe wie bei der Kontrolle durch den Arbeitgeber selbst. Eine Ausübung der Kontrollbefugnisse hängt maßgeblich von einer entsprechenden arbeitsvertraglichen oder kollektivarbeitsrechtlichen Grundlage ab.¹⁵

13 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 47 unter Verweis auf: Schneider, ZD 2011, 153 (155); Herrmann/Zeidler, NZA 2017, 1499 (1500).

14 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 50.

15 Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 56 ff.