Die Folgen der Vernetzung

Connected Car im Arbeitsverhältnis | Wie wirkt es sich auf Arbeitsverträge aus, wenn aus dem Dienstwagen ein Smart Car wird, das mit seiner Umgebung, dem Hersteller, dem Arbeitgeber und Dritten kommuniziert?

Foto: Nito/Fotolia

Intransparenter Datentransfer | Selbst in Kleinwagen gehört die Verbindung mit dem Smartphone via Bluetooth zum Standard. Zuweilen werden auch Adressbücher und Telefonlisten im Wagen gespeichert, selbst wenn das Smartphone nicht verbunden ist

— Das vernetzte Auto ist nicht mehr aufzuhalten: Tesla rollt für sein Model S das autonome Fahren per Software-Update aus, Volvo will die Haftung für selbstfahrende Autos übernehmen und Stuttgart schickt sich an, neben einer Autobahn auch eine Stadtstrecke für Tests mit intelligenten Fahrzeugen freizugeben.

Kaum thematisiert wird jedoch, wie es sich auf Arbeitsverträge auswirkt, wenn aus dem Dienstwagen ein Smart Car wird, das mit seiner Umgebung, dem Hersteller, dem Arbeitgeber und Dritten kommuniziert.

Bislang übliche Dienstwagenregelungen werden den Anforderungen digitalisierter Fortbewegungsmittel nicht gerecht, gleich ob es sich um individuelle Nutzungsverträge, allgemeine Dienstwagenrichtlinien oder Betriebs-/Dienstvereinbarungen mit Betriebs-/Personalrat handelt.

Online-Dienste im Kfz | Online-Dienste stehen mit allen Funktionalitäten im Fahrzeug nur bereit, wenn nach der Registrierung beim Anbieter (in der Regel Hersteller des Fahrzeugs) ein personalisierter, an das jeweilige Fahrzeug gebundener Benutzer-Account eingerichtet wird. Mit diesem Account können zum Beispiel E-Mail- und Social-Media-Zugriffe im Wagen konfiguriert, Routenplanungen aus dem Internet ans Fahrzeug gesendet oder das Auto lokalisiert werden. Im Account sammeln sich so personenbezogene Daten über den Fahrer, aber auch unternehmensbezogene Informationen, zum Beispiel Fahrtziele und betriebliche E-Mails.

Zu klären ist deshalb:

- Wer darf Benutzer-Accounts für Online-Dienste anlegen und wer trägt die Kosten dafür?
- Welche Funktionalitäten dürfen von wem genutzt werden?
- Welche Zugangsrechte hat der Arbeitgeber zu den Benutzer-Accounts?
- Wer ist für die Löschung bei Rückgabe des Fahrzeugs verantwortlich?

Es empfiehlt sich, fahrzeugbezogene Accounts stets auf den Arbeitgeber anzulegen und dem Arbeitnehmer diese für „sein" Fahrzeug zugänglich zu machen. Bei Pool-Fahrzeugen sollte wegen der wechselnden Nutzung auf an das Fahrzeug gebundene Online-Dienste verzichtet werden, um komplexe datenschutz- und arbeitsrechtliche Fragen zu vermeiden.

Smartphones, Car Play und Android Auto | Bereits in Kleinwagen gehört die Verbindung von Smartphone und Fahrzeug via Bluetooth zum Standard. Der Austausch beschränkt sich meist auf Telefon und Audioplayer. Allerdings werden zuweilen auch Adressbücher und Telefonlisten im Wagen gespeichert, selbst wenn das Smartphone nicht verbunden ist.

Viel weiter in der Verbindung von Smartphone und Fahrzeug gehen Car Play und Android Auto: Hierüber kann grundsätzlich jede App ins Auto gebracht werden. Zwar sollen diese Services der größten Smart-

phone-Betriebssystemhersteller Apple (iOS) und Google (Android) die Kommunikation mit dem Internet ohne Umweg über die Technik hinter der Onboard-Unit des Autos erlauben. Unklar ist jedoch, ob und welche Daten zu diesem Zweck im Fahrzeug (zwischen-)gespeichert werden und welchen Umweg Daten über Server der Diensteanbieter nehmen. Porsche hat etwa angekündigt, Android Auto wegen ungeklärter Datenschutzfragen zunächst nicht zu implementieren.

Zu regeln ist deshalb:

- Dürfen Smartphones mit dem Fahrzeug verbunden werden?
- Welche Funktionalitäten dürfen vom Smartphone im Wagen genutzt werden?
- Falls Daten im Auto gespeichert bleiben: Wer löscht diese nach Beendigung der Nutzung?

Werden bei der Kopplung keine Daten im Wagen gespeichert, ist eine großzügige Freigabe unproblematisch. Bei einer (Zwischen-) Speicherung von Daten oder deren Transport über Server eines Diensteanbieters sollte unter Einbeziehung des betrieblichen Datenschutzbeauftragten geprüft werden, welche technischen und organisatorischen Maßnahmen erforderlich sind, um dem Datenschutz bei Nutzung dieser Dienste Rechnung zu tragen.

Autonomes Fahren | Vernetztes Fahren ist nicht mit autonomem Fahren gleichzusetzen. Autonomes Fahren als selbstständiges Steuern eines Fahrzeugs ohne Fahrereingriffe funktioniert allein mit den im Fahrzeug zur Verfügung stehenden Ressourcen. Die Vernetzung unterstützt das autonome Fahren, indem durch den Rückgriff auf externe Quellen die Grundlagen für die fahrerischen „Entscheidungen" des Fahrzeugs verbessert und Informationen an Umsysteme zurückgegeben werden.

Rechtlich völlig ungeklärt ist, wer für Fehlverfahren eines autonom agierenden Autos einstehen muss. Bereits deshalb sollte unmissverständlich geklärt sein, ob und welche Fahrassistenzsysteme in welchem Umfang von Arbeitnehmern genutzt werden dürfen.

Zugleich obliegt dem Arbeitgeber eine Schutzpflicht für den Arbeitnehmer, konkretisiert unter anderem in der DGUV Vorschrift 70 (vormals BGV D 29). Nach § 34 DGUV Vorschrift 70 hat der Arbeitgeber dafür zu sorgen, dass die Betriebsanweisungen des Kfz-Herstellers befolgt und „besondere Regeln" zur Verhütung von Unfällen beachtet werden, die der Arbeitgeber vorgibt. Zugleich muss der Arbeitnehmer nach § 36 DGUV Vorschrift 70 „vor Beginn jeder Arbeitsschicht die Wirksamkeit der Betätigungs- und Sicherheitseinrichtungen" prüfen.

Festlegen sollte der Arbeitgeber deshalb:

- Welche Assistenzsysteme dürfen genutzt werden?
- Wie wird der Arbeitnehmer in der Bedienung geschult und die Schulung dokumentiert?
- Wie haftet der Arbeitnehmer bei Unfällen nach Verwendung von Assistenzsystemen?
- Wer darf zu welchem Zweck Daten aus der Verwendung von Assistenzsystemen auswerten?

Zu beachten ist, dass beim Umgang mit Assistenzsystemen, insbesondere wenn diese Daten in einer für den Arbeitgeber verwertbaren Form protokollieren, der Personal- oder Betriebsrat Mitbestimmungsrechte haben kann. Er sollte deshalb frühzeitig informiert und beteiligt werden.

Das gilt ebenso für Arbeitssicherheitsbeauftragte, gegebenenfalls im Unternehmen tätige Fuhrparkleiter sowie den Einkauf, der besondere Anforderungen bei der Konfiguration der Dienstwagen zu beachten hat.

Der Einsatz von Tools für den Zugriff auf Kfz-Daten sollte für Arbeitnehmer verboten sein.

Zugriff auf Kfz-Daten | Viele Fahrzeuge verfügen über Schnittstellen zu ihren internen Systemen, über die Daten zum Fahrzeug und Fahrverhalten auch während der Fahrt abgegriffen werden können. Ein Beispiel sind die sogenannten ODB2-Adapter, die über passende Apps Diagnose-Informationen auslesen, ebenso Tools, mit denen sich die Bordelektronik umprogrammieren lässt, zum Beispiel um vom Hersteller zu Testzwecken vorgesehene Funktionalitäten freizuschalten.

Festzuhalten ist dabei:

- Dürfen Schnittstellen im Fahrzeug für Diagnose- oder Programmier-Tools genutzt werden?
- Welche Tools dürfen von wem zu welchem Zweck eingesetzt werden?
- Wer haftet bei Fehlern in den Tools oder bei deren Benutzung?

Problematisch ist bei solchen Tools stets, ob diese und der Anwender über die erforderliche technische Sicherheit beziehungsweise Erfahrung verfügen. Idealerweise wird der Einsatz solcher Tools für den Zugriff auf Kfz-Daten deshalb Arbeitnehmern verboten. Nur im Einzelfall, beispielsweise bei Beschäftigten in eigenen Werkstätten, kann hiervon eine Ausnahme gemacht werden.

Privatnutzung | Üblicherweise werden Dienstwagen als Statusfahrzeuge zur privaten Nutzung durch den Fahrer und meist auch dessen Familienangehörige, seltener auch beliebigen Dritten überlassen. Hierbei ist auf eine Widerspruchsfreiheit der Dienstwagenregeln zu anderen Richtlinien und Vereinbarungen zu achten.

Oftmals ist etwa die private Nutzung betrieblicher IT verboten. Gehört zur betrieblichen IT auch ein Smartphone und darf der Arbeitnehmer dies mit dem Kfz verbinden, ist es praktisch unmöglich, diese Verbindung automatisch während privater Fahrten aufzuheben. Dann aber nutzt der Arbeitnehmer das Smartphone privat während einer privaten Fahrt, obwohl ihm nur das private Fahren, nicht aber das private „Mitnutzen" des Smartphone gestattet ist. Das lässt sich durch entsprechende Ausnahmen in den IT-Richtlinien in den Griff bekommen.

Besonderer Beachtung bedarf auch der Umgang mit aus dem Fahrzeug erhobenen und vom Arbeitgeber verarbeiteten und genutzten personenbezogenen Daten, wenn diese aus der Freizeit des Arbeitnehmers stammen oder gar Familienangehörigen oder Dritten gehören. Hier sind gegebenenfalls Einwilligungen vom Arbeitnehmer und den Dritten einzuholen, um einen datenschutzkonformen Umgang mit solchen „privaten" Daten sicherzustellen.

Dash-Cams | Bei dieser Gelegenheit kann zugleich der Einsatz von Dash-Cams verboten werden. Sie sind rechtlich problematisch, weil sie personenbezogene Daten und Videoaufnahmen ohne Einwilligung der Betroffenen anfertigen. Duldet der Arbeitgeber den Einsatz von Dash-Cams, kann er hierdurch in die rechtliche Verantwortlichkeit für die während der Dienstfahrten entstandenen Aufnahmen geraten. Dies wird mit einem Verbot vermieden.

| Sascha Kremer

Sascha Kremer | Fachanwalt für IT-Recht bei Login Partners, Pulheim, sowie externer Datenschutzbeauftragter, Datenschutzauditor und Lehrbeauftragter