DATENSCHUTZ

Wissen, was zu tun ist

Noch immer wirft das Thema Datenschutzgrundverordnung viele Fragen in der Praxis auf. Tipps für den Werkstattalltag von der Kanzlei RAW – Partner WPG.

Fotos: stockpics/stock.adobe.com, RAW

Die Datenschutzvorgaben der DSGVO sollen kleine Unternehmen nicht überfordern.

Vor dem Hintergrund allgegenwärtiger Datenverarbeitung hat die Bedeutung des Datenschutzes zugenommen. Diesen Stellenwert von Daten hat die EU schon vor dem Facebook-Datenskandal erkannt und mit Wirkung zum 25.05.2018 die neue EU-Datenschutzgrundverordnung (EU-DSGVO) eingeführt. Auch für Kfz-Werkstätten sind datenschutzrechtliche Sachverhalte an der Tagesordnung und werden in Zukunft noch wichtiger – sei es die Verarbeitung von Kundendaten bei Reparatur- und Inspektionsaufträgen oder der Umgang mit den Daten von den eigenen Mitarbeitern.

Anwendungsbereich der EU-DSGVO

Die EU-DSGVO findet unabhängig von der Größe des Betriebs Anwendung, sobald eine Kfz-Werkstatt personenbezogene Daten verarbeitet. Personenbezogene Daten sind all diejenigen Merkmale, anhand derer eine natürliche Person erkannt werden kann. Solche Merkmale sind:

- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usw.),
- Kennnummern (Sozialversicherungs- und Steueridentifikationsnummer, Nummer bei der Krankenversicherung, Personalausweisnummer usw.),
- Bankdaten (Kontonummern, Kreditinformationen, Kontostände usw.),
- Online-Daten (IP-Adresse, Standortdaten usw.),
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usw.),
- Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten usw.),
- Kundendaten (Bestellungen, Adressdaten, Kontodaten usw.),
- Werturteile (Schul- und Arbeitszeugnisse usw.).

Grundsätze der EU-DSGVO

Personenbezogene Daten sollen nach der EU-DSGVO durch folgende Grundsätze geschützt werden:

- Rechtsmäßigkeit, d.h. eine Datenverarbeitung soll nur mit Einwilligung oder bei besonderem Interesse erfolgen;
- Verarbeitung nach Treu und Glauben, d.h. mit den Daten ist vernünftig, transparent und einfach nachvollziehbar umzugehen;
- Zweckbindung, d.h. der Zweck der Datenverarbeitung muss festgelegt, eindeutig und legitim sein;
- Datenminimierung, d.h. Verarbeitung personenbezogener Daten muss auf das notwendige Maß beschränkt sein;
- Richtigkeit, d.h. nur richtige personenbezogene Daten dürfen verwendet und unrichtige müssen unmittelbar gelöscht oder korrigiert werden;
- Speicherbegrenzung, d.h. personenbezogene Daten dürfen nur solange gespeichert werden, wie es für die Verwendung und den Zweck erforderlich ist;
- Integrität und Vertraulichkeit, d.h. angemessene Sicherheit der personenbezogenen Daten durch Schutz vor unbefugtem Zugriff und Verarbeitung;
- Rechenschaftspflicht, d.h. die Einhaltung der vorgenannten Grundsätze muss durch das Unternehmen nachgewiesen werden.

EU-DSGVO für Kfz-Betriebe

Jedes Unternehmen, in dem zehn oder mehr Personen ständig mit der Bearbeitung personenbezogener Daten mittels EDV beschäftigt sind, muss einen Datenschutzbeauftragten bestellen. Ständig

KURZFASSUNG

Kein Betrieb muss Angst haben vor der seit Mai geltenden Datenschutzgrundverordnung. Der vorliegende Beitrag weist auf die insbesondere für den Werkstatt-Alltag relevanten Punkte hin. Es wird nichts verlangt, was für Betriebe nicht leistbar wäre.

beschäftigt sind solche Personen, die permanent mit Kunden- und Personaldaten zu tun haben, in der Regel also vor allem Bürokräfte, die Personal- und Kundenverwaltung im Betrieb übernehmen. Mechatroniker zählen nicht mit, wenn sie lediglich bei Reparaturen mittels Computer Fehler aus dem Speicher des Fahrzeugs auslesen und identifizieren.

Verarbeitungsverzeichnisse

Unabhängig von der Mitarbeiterzahl muss jede Kfz-Werkstatt ein Verarbeitungsverzeichnis führen. In dieses Verzeichnis sind folgende Angaben/Vorgänge aufzunehmen:

- durchgeführte Datenverarbeitungstätigkeit und der dafür verantwortliche Mitarbeiter,
- Beginn der Datenverarbeitungstätigkeit,
- Zwecke der Datenverarbeitung,
- betroffener Personenkreis,
- aufgezeichnete personenbezogene Daten,
- Empfänger personenbezogener Daten,
- Löschfristen sowie technische und/oder organisatorische Maßnahmen.

Bei einer Kfz-Werkstatt sind in dieses Verzeichnis insbesondere, aber nicht abschließend, folgende Vorgänge aufzunehmen: Lohnabrechnung, Bewerbungsverfahren, IT-Support, Betrieb der Firmenwebseite, Personalverwaltung, Kunden- und Auftragsverwaltung sowie Auswertung von Fahrzeugdaten.

Blick auf die IT-Sicherheit

IT-Sicherheit im Sinne der EU-DSGVO bedeutet, die Daten mittels technischer und organisatorischer Maßnahmen, abgekürzt TOM, zu schützen. Technische Maßnahmen sind alle Maßnahmen, die sich physisch umsetzen lassen, zum Beispiel durch das Installieren einer Alarmanlage oder Benutzerkonten, die passwortgeschützt sind. Organisatorische Maßnahmen beziehen sich auf die Rahmenbedingungen des Datenverarbeitungsvorgangs. Sie umfassen Regeln, Vorgaben und Handlungsanweisungen, die dazu dienen, dass Mitarbeiter den Datenschutz gesetzestreu einhalten, beispielsweise durch einen IT-Leitfaden. Bei all diesen Maßnahmen darf aber gemäß der EU-DSGVO berücksichtigt werden, dass gerade von kleinen und mittelgroßen Kfz-Werkstätten kein unverhältnismäßiger Aufwand verlangt werden darf.

Einwilligungserklärungen

Wie bereits vor der EU-DSGVO waren Einwilligungserklärungen einzuholen, bevor Telefonnummern, Fotos und E-Mail-Adressen von Mitarbeitern im Internet veröffentlicht, für Kunden Einträge in Kontaktformulare auf einer Webseite oder der Bezug eines Newsletters ermöglicht werden durften. Die Einwilligungserklärungen sollten ausreichend dokumentiert werden. Entsprechend sollten die Datenschutzhinweise mit Informationen zur Verarbeitung personenbezogener Daten auf den Webseiten an die neuen Vorschriften angepasst werden. Inhaltlich müssen Datenschutzhinweise und vorformulierte Einwilligungserklärungen in klarer und einfacher Sprache über Zwecke, Art, Umfang und Dauer der Datenspeicherung informieren. Dabei muss über die Möglichkeit des Widerrufs der Einwilligung aufgeklärt werden.

Auftragsdatenverarbeitung

Werden im Auftrag der Kfz-Werkstatt personenbezogene Daten durch externe Dienstleister verarbeitet, muss die Kfz-Werkstatt zunächst prüfen, ob der Beauftragte geeignet ist, die Dienstleistung in Übereinstimmung mit der EU-DSGVO zu erbringen. Als externe Dienstleister kommen insbesondere Anbieter von Werkstattsoftware oder externe IT-Administratoren in Betracht. Im Anschluss an die Überprüfung muss mit dem externen Dienstleister ein schriftlicher oder elektronischer Vertrag über die Auftragsverarbeitung abgeschlossen werden. Wichtige Inhalte sind Regelungen zur Bereitstellung der Daten, Einhaltung besonderer Bedingungen für Subunternehmer und Sicherheit der personenbezogenen Daten.

Haben Sie Ihre Lohn- und Gehaltsbuchhaltung an einen Steuerberater ausgelagert, dann müssen Sie mit Ihrem Steuerberater keinen neuen Vertrag schließen, da der Steuerberater kein Auftragsdatenverarbeiter ist.

Aufbewahrung und Löschung

Die Vorgehensweise zur Aufbewahrung und Löschung personenbezogener Daten muss in einem gesonderten Konzept dokumentiert werden. Dabei können sich unterschiedliche Aufbewahrungsfristen für Daten ergeben. Besteht ein Rechtsstreit mit früheren Kunden oder ehemaligen Mitarbeitern, so können relevante Daten bis zur Beendigung des Rechtsstreits aufbewahrt werden. Soweit Unterlagen von Kunden und Mitarbeitern für Besteuerung und Bilanz wichtig sind, müssen diese entsprechend den gesetzlichen Aufbewahrungsfristen von Handels- und Steuerrecht bis zu 10 Jahre aufbewahrt werden.

Meldepflicht bei Datenpanne

Datenschutzverletzungen müssen grundsätzlich innerhalb von 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde für Datenschutz gemeldet werden. Dies gilt nur dann nicht, wenn die Kfz-Werkstatt darlegen kann, dass die Verletzung voraussichtlich nicht zu einem Risiko für Kunden oder Mitarbeiter führt. Kann das Risiko nicht verlässlich eingeschätzt werden, sollte vorsorglich eine Meldung erfolgen.

Information der eigenen Mitarbeiter

Datenschutz gilt nicht nur für Kunden, sondern insbesondere auch für die eigenen Mitarbeiter. So müssen Sie Mitarbeiter informieren, was mit ihren personenbezogenen Daten passiert. Ist die Lohn- und Gehaltsbuchhaltung an einen Steuerberater ausgelagert, so müssen Sie Ihre Mitarbeiter darüber informieren.

Joachim Will
Rechtsanwalt, Steuerberater
www.raw-partner.de

KOMMENTAR

Der Datenschutz sollte nicht auf die leichte Schulter genommen werden. Die EU hat erkannt, wie wichtig und schutzwürdig heutzutage personenbezogene Daten sind. Welcher von den konkreten Schritten noch eingeleitet werden muss, hängt insbesondere von der Größe des Betriebs und den bisherigen Strukturen ab. Wurden bislang Datenschutzverstöße eher milde sanktioniert, können Bußgelder bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes auferlegt werden. Um solchen Sanktionen zu entgehen, ist hier dringend Vorsicht und gegebenenfalls Anpassungsarbeit geboten!

Maximilian Appelt
Rechtsanwalt, Steuerberater