

Wenn ein Diagnosegerät oder Abgastester von Hella Gutmann in Ihrer Werkstatt verwendet wird, müssen Sie einen Auftragsverarbeitungsvertrag mit der Hella Gutmann Solutions GmbH abschließen. Um Ihnen die Erstellung eines solchen Vertrags zu ersparen, haben wir diesen für Sie verfasst. Der Auftragsverarbeitungsvertrag ist dem Anhang dieser E-Mail beigefügt oder kann auf der Homepage www.hella-gutmann.com/privacy heruntergeladen werden. Sie müssen lediglich noch die Firmierung ihrer Werkstatt einfügen und den Vertrag unterzeichnet an av-vertrag@hella-gutmann.com schicken. Ebenso muss auch mit allen anderen Unternehmen, an die personenbezogene Daten übermittelt werden, ein Auftragsverarbeitungsvertrag geschlossen werden.

WAS MUSS BEI DER SPEICHERUNG UND NUTZUNG VON PERSONENBEZOGENEN DATEN BEACHTET WERDEN?

Ein wichtiges Ziel des Datenschutzes ist den Missbrauch von personenbezogenen Daten zu verhindern. Durch Eingriffe in ungesicherte IT-Systeme können kriminelle Bankdaten abgreifen und so unbefugt auf Konten zugreifen. Mit Personal- oder Ausweisnummern können sie falsche Dokumente erstellen und verkaufen. Der Missbrauch personenbezogener Daten hat oftmals einen wirtschaftlichen Hintergrund. Deswegen ist es umso wichtiger datenschutzkonform mit den Daten umzugehen. Das heißt, wir müssen unsere Mitarbeiter auf das Datengeheimnis verpflichten, unsere IT-Systeme regelmäßig mit der neusten Sicherheitssoftware ausstatten, Daten nur über verschlüsselte Kanäle versenden und unsere Computer wie auch Diagnosegeräte durch einen Passwortschutz vor unbefugten Eingriffen sichern. Zudem müssen wir Daten in Papierform in geeigneten Schließfächern aufbewahren und personenbezogene Daten löschen, wenn der Zweck ihrer Erhebung wegfällt. Das sind mitunter die wichtigsten Vorgaben der Gesetzgebung, um die Datensicherheit zu gewährleisten.

Die Hella Gutmann Solutions GmbH nutzt für die Übertragung von Daten über das Diagnosegerät angemessene Verschlüsselungsprogramme um ihre Daten vor Hackerangriffen zu schützen. Zukünftig wird Ihnen auch eine Passwortschutzfunktion für das Diagnosegerät zur Verfügung stehen.

WELCHE BUSSGELDER DROHEN, WENN DIE REGELUNGEN NICHT EINGEHALTEN WERDEN?

Die maximale Geldbuße liegt bei 20 Millionen Euro oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist. Natürlich sind solche Beträge weit entfernt von der Realität einer mittelständischen Werkstatt, sie sind aber auch nur die höchstmögliche Strafe bei Missachtung der gesetzlichen Vorschriften. Experten erwarten, dass die neuen Bußgelder bei ca. 30.000 Euro beginnen werden und das kann auch schon ganz schön wehtun.

AB DEM 25. MAI 2018 GILT DIE NEUE EU-DATENSCHUTZ-GRUNDVERORDNUNG

NOCH EINMAL ALLES IN KÜRZE

WAHLLOSE SPEICHERUNG VON KUNDEN- ODER MITARBEITERDATEN IST VERBOTEN.

Für viele Situationen im Arbeitsalltag benötigen wir personenbezogene Daten wie z. B. den Namen des Kunden um einen Auftrag entgegen zu nehmen, die VIN zum Auslesen von Fahrzeugdaten oder Kontodaten eines Mitarbeiters für die Überweisung des Gehalts. Alle diese Daten sind das Eigentum der entsprechenden Personen. Wir dürfen sie nur verwenden zur Erfüllung von rechtlichen Pflichten und zur Wahrung unserer Geschäftszwecke oder wenn der Eigentümer der Nutzung zugestimmt hat. Ansonsten dürfen keine personenbezogenen Daten gespeichert oder genutzt werden.

DATEN VON KUNDEN ODER MITARBEITERN SIND NUR GEBORGT.

Wenn wir personenbezogene Daten speichern, müssen wir jederzeit wissen, wo sich die Angaben befinden und was damit gemacht wird. Denn die Daten sind nur geborgt. Jeder Kunde wie auch Mitarbeiter hat das Recht zu erfahren, welche Daten wir über ihn/sie besitzen. Darüber hinaus können die Eigentümer ihre Daten zurückverlangen bzw. ihre Löschung fordern, wenn keine rechtlichen Gründe dagegensprechen.

VORSICHT BEI DER WEITERGABE VON PERSONENBEZOGENEN DATEN.

In den wenigsten Fällen werden erhobene Daten nur innerhalb des Unternehmens genutzt. Häufig übernimmt zum Beispiel der Steuerberater auch die Gehaltsabrechnung oder die eingesetzten IT-Systeme speichern automatisch Daten in einer Cloud. Wenn wir solche Dienste nutzen, geben wir personenbezogenen Daten an Dritte weiter. Gesetzlich erlaubt ist die Weitergabe nur zur Erfüllung der Vertragspflichten. Gleichzeitig sind wir in solchen Fällen dazu verpflichtet unsere Kunden bzw. Mitarbeiter darüber zu informieren und einen Auftragsverarbeitungsvertrag mit dem entsprechenden Dienstleister abzuschließen. Wollen wir die personenbezogenen Daten auch für anderen Zwecke weitergeben, brauchen wir das Einverständnis des Dateneigentümers.

SICHERHEIT STEHT AN OBERSTER STELLE.

Wenn uns personenbezogenen Daten anvertraut werden, müssen wir damit sehr sorgfältig umgehen. Deshalb sind alle Daten so aufzubewahren, dass niemand Unbefugtes auf sie zugreifen kann. Das heißt auch, dass wir unsere Computer regelmäßig mit der neusten Sicherheitssoftware ausstatten und uns ausloggen, wenn wir den Rechner oder das Diagnosegeräte nicht verwenden.



**WICHTIGE TIPPS,
DAMIT SIE BESCHIED WISSEN**



**PRAKTISCHER GUIDE
ZUM DATENSCHUTZ**

HELLA GUTMANN SOLUTIONS GMBH

Am Krebsbach 2 | D-79241 Ihringen | Tel.: +49 (0) 7668-9900-0

E-Mail: personal@hella-gutmann.com | www.hella-gutmann.com

Der Grund warum Sie gerade diese Informationsbroschüre in den Händen halten, ist die neue EU-Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 in Kraft tritt. Unsere Gesetzgebung verwendet in ihren Vorschriften häufig eine umständliche Sprache, die in vielen Fällen schwer zu lesen und zu verstehen ist. Aus diesem Grund haben wir einige der wichtigsten Vorschriften für Sie in der Alltags-sprache zusammengefasst.

Als erstes ist es uns wichtig darauf hinzuweisen, dass es beim Datenschutz immer nur um PERSONENBEZOGENE Daten geht. Relevant sind somit nur Daten auf Basis derer man eine Person identifizieren kann. Darunter fallen zum einen Daten die direkt auf eine Person hinweisen, wie zum Beispiel Name, Adresse, Telefonnummer und zum anderen Daten, die mit Hilfe von Zusatzwissen auf eine Person schließen lassen. Dazu zählen beispielsweise die Personalnummer, das Kennzeichen oder die VIN.

TYPISCHE PERSONENBEZOGENE DATEN DER MITARBEITER:

- Name, Adresse
- E-Mail, Telefonnummer
- Personalnummer
- Bankverbindung
- Gesundheitsbezogene Angaben
- Bewerbungsunterlagen

TYPISCHE PERSONENBEZOGENE DATEN DER WERKSTATTKUNDEN:

- Name, Adresse
- Telefonnummer, E-Mail
- Kreditkartenangaben
- Führerschein
- Kennzeichen, VIN

VERMEIDEN SIE HOHE GELDSTRAFEN UND ENTtäUSCHTE KUNDEN

Die neue EU-Datenschutz-Grundverordnung verbietet nicht personenbezogenen Daten zu erheben und zu verarbeiten, sondern schreibt vor, wie wir damit umzugehen haben. Etwa 80 % der Regelungen zum Datenschutz sind schon heute gültig. Jedoch wissen die wenigsten, was man darf und was nicht. Genau hier möchten wir mit dieser Broschüre Licht in die Sache bringen.



WANN DÜRFEN WIR PERSONENBEZOGENE DATEN SPEICHERN UND NUTZEN?

Es gibt unterschiedliche Situationen im Arbeitsalltag, in denen es uns möglich sein muss, personenbezogene Daten zu verarbeiten. Wenn wir zum Beispiel einem Kunden eine Inspektion oder Reparatur in Rechnung stellen, benötigen wir den Namen und die Adresse des Kunden. Wir müssen auch den Führerschein sehen, bevor wir ihm oder ihr einen Leihwagen geben können. Wir benötigen die VIN um das korrekte Fahrzeug auszuwählen. Und um das Gehalt unserer Mitarbeiter auszahlen zu können, brauchen wir ihre Kontodaten. Wäre die Speicherung und Verarbeitung dieser Daten verboten, könnten wir unseren Vertragspflichten nicht nachkommen oder unseren Geschäftszweck nicht verfolgen. Damit wir das aber können erlaubt die Gesetzgebung die Speicherung und Nutzung personenbezogener Daten für solche Zwecke. Allerdings wird von uns gefordert, dass wir ein Verzeichnis darüber führen, welche personenbezogenen Daten wir haben, und wozu wir sie brauchen.

Möchten wir hingegen für andere Zwecke personenbezogenen Daten speichern und nutzen, brauchen wir die Zustimmung des Kunden bzw. des Mitarbeiters. Wenn wir beispielsweise die Telefonnummern unserer Kunden verwenden, um sie über Angebote zu informieren, brauchen wir ihre Erlaubnis dazu. Das gilt auch, wenn wir die Daten über ihre familiären Verhältnisse speichern, um eine bessere Kunden-nähe zu erzielen. Es empfiehlt sich die Zustimmung immer schriftlich einzuholen, um sie nachweisen zu können. Besonders sensible Daten, wie die politische oder religiöse Überzeugung oder die genetische Veranlagung unserer Mitarbeiter oder Kunden, sollten wir niemals abfragen. Es gibt nur sehr wenige Fälle in denen diese Informationen wirklich notwendig sind. Und in den Werkstätten sind diese eigentlich nie vorzufinden. Als Leitplanke können wir uns merken, personenbezogene Daten dürfen nur dann erhoben und verarbeitet werden, wenn wir sie zu einem sachlichen und relevanten Zweck benötigen.

WER IST DER EIGENTÜMER DER DATEN?

Die EU-Datenschutz-Grundverordnung hebt deutlich hervor, dass jeder EU-Bürger der Eigentümer aller seiner Daten ist. Somit sind die personenbezogenen Daten, die wir erheben und nutzen nur geborgt. Jeder EU-Bürger hat das Recht zu erfahren, welche Daten wir über ihn haben und wofür wir diese nutzen. Deshalb sind wir dazu verpflichtet ihm Auskunft zu geben, wenn er darum bittet. Zudem kann er seine Daten von uns zurückverlangen bzw. ihre Löschung fordern, wenn keine rechtlichen Gründe dagegensprechen. Wenn wir die Erlaubnis eines Kunden oder Mitarbeiters haben, seine personenbezogenen Daten zu nutzen, kann er diese jederzeit widerrufen. Auch hier sind wir dazu verpflichtet seinem Wunsch nachzugehen. Wenn wir zur Erfüllung unserer Vertragspflichten personenbezogene Daten an Dritte weitergeben, haben wir die Pflicht ihn über den Zweck und Umfang der Übermittlung zu informieren.

WAS IST BEI DER WEITERGABE VON PERSONENBEZOGENEN DATEN AN DRITTE ZU BEACHTEN?

In den wenigsten Fällen werden erhobene Daten nur innerhalb des Unternehmens genutzt. Wenn wir zum Beispiel Mitarbeiterdaten an den Steuerberater für die



Gehaltsabrechnung versenden oder wenn unsere IT-Systeme (EDV-Lösung, Diagnosegerät) automatisch Daten in einer Cloud speichern, leiten wir Daten an Dritte weiter. Hierbei müssen die folgenden vier Punkte Berücksichtigt werden.

- **Erstens:** Die Weitergabe von personenbezogenen Daten, ohne eine Zustimmung des Eigentümers, ist nur zur Erfüllung der Vertragspflichten erlaubt. Das heißt, wenn wir mit dem Kunden eine Reparatur des Autos vereinbart haben und dafür ein Diagnosegerät benötigen, brauchen wir hier nicht die Zustimmung des Kunden, weil wir für die Reparatur bzw. zur Erfüllung des Vertrages das Diagnosegerät verwenden müssen. Sonst wäre die Reparatur nicht möglich. Für solche Fälle ist eine gesonderte Zustimmung nicht notwendig.
- **Zweitens:** In einem solchen Fall muss der Dateneigentümer einmalig darüber informiert werden.
- **Drittens:** Wir müssen mit dem externen Dienstleister einen Auftragsverarbeitungsvertrag abschließen, um sicherzustellen, dass das Unternehmen datenschutzkonform mit den anvertrauten Daten umgeht.
- **Viertens:** Wollen wir die personenbezogenen Daten auch für andere Zwecke weitergeben, brauchen wir das Einverständnis des Dateneigentümers.

AUFTRAGSVERARBEITUNGSVERTRAG.

Wenn wir personenbezogenen Daten an andere Unternehmen weiterleiten, werden wir vom Gesetzgeber als **Datenverantwortlicher** definiert. Das andere Unternehmen hingegen ist der **Datenverarbeiter**. Als Datenverantwortlicher müssen wir uns vergewissern, dass der Datenverarbeiter die übermittelten Daten korrekt verarbeitet. Dies wird durch einen Auftragsverarbeitungsvertrag gewährleistet, der zwischen dem Datenverantwortlichen und dem Datenverarbeiter geschlossen werden muss. In diesem Vertrag sind zum einen alle Zwecke der Datenübermittlung aufzulisten. Zum anderen müssen die technischen und organisatorischen Maßnahmen des Datenverarbeiters dem Vertrag als Anlage beigefügt werden, die die Maßnahmen zur Erfüllung der Sicherheits- und Schutzanforderungen beschreiben.