DATENSCHUTZ - D01a

Stand: Mai 2018

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

EU-Datenschutz-Grundverordnung für kleine Unternehmer und Existenzgründer - Praktisches Fallbeispiel -

Gesetzestexte sind - auch für Juristen - nicht immer leicht zu verstehen. Deshalb möchten wir Ihnen anhand eines praktischen Falls die Umsetzung der DSGVO näher bringen.

Unser Fallbeispiel:
Einzelunternehmerin Miranda Mustera, „Homedreams“, Geschäftszweig: Einzelhandel mit Wohnaccessoires und Möbeln, Angebot von Stilberatungskursen; MitarbeiterInnen: 4.

Was muss sie tun, um sich datenschutzkonform zu verhalten?

I. Rechtsgrundlage für die Datenverarbeitung

1. Vertrag mit ihren Kunden

Wenn Frau Mustera ihren Kunden etwas verkaufen oder eine Dienstleistung erbringen will, handelt es sich um die Anbahnung bzw. Erfüllung eines Vertragsverhältnisses. Hierzu benötigt sie entsprechende Angaben ihrer Kunden (z. B. Name, Anschrift, Telefonnummer). Darüber hinausgehende Angaben wie E-Mail-Adresse, Geburtsdatum (für Glückwunschbriefe), Kaufinteressen, Teilnahme(interesse) an Kursen und Fotos von TeilnehmernInnen) sind hingegen nicht erforderlich für die Erfüllung des Vertrags.

Für die Grunddaten zur Abwicklung des Vertrags benötigt Frau Mustera keine gesonderte Einwilligung ihrer Kunden, für darüber hinausgehende Daten aber schon. Falls der Vertrag erfüllt ist und es keine gesetzlichen Gründe für seine Aufbewahrung mehr gibt (z. B. steuerliche oder handelsrechtliche Gründe), müssen die Daten gelöscht werden.

2. Einwilligung ihrer Kunden
Für personenbezogene Daten, die nicht für die Vertragserfüllung benötigt werden, muss Frau Mustera eine Einwilligung einholen. In der Einwilligungserklärung muss sie auf die jederzeitige Widerrufbarkeit dieser Einwilligung hinweisen. Sie sollte hier nach obligatorischen und freiwilligen Daten trennen. Frau Mustera kann eine elektronische Einwilligung einholen, darf aber keine voreingestellte Einwilligung in Form eines Häkchens verwenden („double-opt-in"). Zudem muss sie ihre Kunden darüber informieren, zu welchem Zweck sie diese Daten verarbeiten will.

Sie muss prüfen, ob die bisherigen Einwilligungen, die sie eingeholt hat, den neuen Anforderungen entsprechen. Falls nicht, wenn also der Hinweis auf den jederzeitigen Widerruf oder die Angabe des Zwecks fehlt, müssen die Einwilligungen neu eingeholt werden.

Sie muss die Einwilligungen dokumentieren.

➔**D02** „Einwilligung nach der DSGVO", **Kennzahl 2158**

Bei der Einholung der Einwilligung von ihren Kunden muss sie nicht nur die datenschutzrechtlichen Anforderungen erfüllen, sondern auch bei einer Einwilligung zur Werbung das Gesetz gegen unlauteren Wettbewerb (UWG) beachten.

➔**W08** „Telefon-, Fax-, E-Mail-und Brief-Werbung", **Kennzahl 65**

3. Sie muss Informationspflichten erfüllen (teilweise neu)

➔**D05** „Informationspflichten", **Kennzahl 2158**

Zu den Informationspflichten gehören:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters: *„Verantwortlicher" ist Frau Mustera als Einzelunternehmerin, sie muss ihre Namen und ihre Kontaktdaten angeben.*
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden): *Frau Mustera ist nicht gesetzlich verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Diese Pflicht greift erst ab 10 Beschäftigten ein.*

  ➔**D06** „Betrieblicher Datenschutzbeauftragter nach der DSGVO und dem BDSG (neu)", **Kennzahl 2158**
- Zwecke der Verarbeitung: *(Lieferung der Möbel)* und Rechtsgrundlage *(Kaufvertrag),*
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht: berechtigtes Interesse des Verantwortlichen: *Kontaktformular im Internet: „Wir benötigen Ihre Daten, um Ihre Anfrage zu beantworten"*,
- ggf. Empfänger oder Kategorien von Empfängern: nur bei Übermittlung anzugeben: „*Wir übermitteln Ihre Kundendaten an unsere Speditionsunternehmen*, *damit Sie Ihre Möbelbestellung erhalten.",*

- Absicht der Übermittlung in ein Drittland/internationale Organisation sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission (nur bei Übermittlung anzugeben),
- Dauer der Datenspeicherung: *Orientierung an steuerrechtlichen Aufbewahrungsfristen,*
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit,
- Recht auf Widerruf einer Einwilligung,

  ➔**D02** „Einwilligung nach der DSGVO“, **Kennzahl 2158**
- Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde,
- Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte.

Diese Informationspflichten müssen zum Zeitpunkt der Erhebung gegenüber dem - zukünftigen - Kunden erfüllt werden. Das funktioniert z. B., wenn der Kunde bei Frau Mustera im Ladengeschäft die Möbel kauft. Dann kann sie ihm ein entsprechendes Datenschutz-Informationsblatt/eine Datenschutzerklärung geben. In ihrem Onlineshop muss sie diese Informationen an zentraler Stelle platzieren.

➔**D07** „Die Datenschutzerklärung nach der DSGVO“, **Kennzahl 2158**

Falls die Daten nicht bei den Kunden direkt erhoben wurden, muss die Quelle angegeben werden: *Ihre Daten haben wir bei XYZ erworben.*

Für die Nutzer ihrer **Internetseite** muss Frau Mustera bekannt geben, ob und welche **Cookies** sie verwendet und ob sie sog. **Analyse- oder Tracking-Tools,** *z.B. Google Analytics,* nutzt. Nutzt sie hierfür einen externen Dienstleister, muss sie dazu eine **Vereinbarung über die Auftragsverarbeitung** schließen. Der *Auftragsverarbeitungs-Vertrag* wird von Frau Mustera aufbewahrt.

➔**D12** „Auftragsverarbeitung nach der DSGVO“, **Kennzahl 2158**

Hat der Dienstleister seinen Sitz in einem Drittland, z. B. den USA, muss sie prüfen, ob die Weitergabe der Daten über EU-Standardvertragsklauseln oder über das sog. Privacy Shield abgesichert ist. Dabei handelt es sich um eine Vereinbarung zwischen der EU und den USA zur Angemessenheit des Datenschutzniveaus bei denjenigen Unternehmen, die die Anforderungen des Privacy Shield erfüllen.

II. Hinzuziehung externer Dienstleister

In der Regel kooperieren Unternehmen mit externen Dienstleistern. Folgende Fälle sind dabei zu beachten:

a) **Wo verarbeitet Frau Mustera diese Daten?** Auf ihrem eigenen Server oder bei einem Dritten? Bei letzterem muss sie eine schriftliche (oder elektronische) Vereinbarung über die Auftragsverarbeitung schließen, denn der IT-Dienstleister darf die Daten nur nach ihrer Weisung verarbeiten. Liegen die Daten auf ihrem eigenen Server, nutzt sie aber eine Cloud-Anwendung, muss sie klären, ob die Daten in Deutschland, in Europa oder in den USA gespeichert sind. Im letzteren Fall handelt es sich um einen Datentransfer in Drittländer, so dass Sie hierfür eine besondere Grundlage benötigen, wenn die Daten in die USA übermittelt werden.

b) Frau Mustera hat einen **Internetauftritt,** der von einer Webdesign-Agentur gestaltet wird. Hat die Webdesign-Agentur Zugriff auf die personenbezogenen Daten, die ihre Interessenten/Kunden dort angeben? Falls ja, muss sie auch hier eine **Vereinbarung über die Auftragsverarbeitung schließen.** Zudem ist sie nach dem Telemediengesetz verpflichtet, ein sogenanntes **Impressum** mit folgenden Angaben zu haben: Name, Anschrift, Rechtsform, E-Mail-Adresse, Umsatzsteuer-Identifikationsnummer usw. [Bei mehr als 10 Beschäftigten muss Frau Mustera zusätzlich angeben, inwieweit sie bereit oder verpflichtet ist, an einem Verfahren vor einer Verbraucherschlichtungsstelle teilzunehmen (§§ 36, 37 Verbraucherstreitbeilegungsgesetz).] Bei Online-Verträgen muss sie ihrer Informationspflicht nach Art. 14 der sog. ODR-Verordnung nachkommen.

   ➔ **R13** „Anbieterkennzeichnung bei einer Firmen-Homepage- Impressum -“, **Kennzahl 44**

   ➔ **R80** „Verbraucherschlichtung: Neue Informationspflichten für Online-Händler“, **Kennzahl 44**

c) Frau Mustera lässt ihre **Buchführung,** insbesondere auch die Gehaltsabrechnung ihrer Mitarbeiter, über einen Steuerberater abwickeln. Hierfür muss sie einen entsprechenden Dienstvertrag schließen.

d) Miranda Mustera schaltet ein **Inkassounternehmen** ein, um säumige Kunden zur Zahlung auffordern zu lassen. Sie muss ihre Kunden darauf aufmerksam machen, dass sie im Falle ausstehender Zahlungen ein Inkassounternehmen mit der Wahrnehmung ihrer Interessen beauftragt: *Wir weisen Sie darauf hin, dass wir im Falle der Nichtzahlung Ihre Kundendaten an ein Inkassounternehmen zur Verfolgung unserer Ansprüche weitergeben.*

e) Frau Mustera nutzt einen **elektronischen Bezahldienst,** mit dem sie einen Auftragsdatenverarbeitungsvertrag schließen muss.

III. Daten von Lieferanten

Miranda Mustera hat Lieferanten, von denen sie ebenfalls Daten wie Name, Anschrift, Telefonnummer, Produktangebot, Ansprechpartner, URL der Homepage und E-Mail-Adressen gespeichert hat. Diese Angaben fallen im Normalfall im Rahmen der Vertragsabwicklung an. Dann ist der Vertrag die Rechtsgrundlage für die Datenverarbeitung.

IV. Mitarbeiterdaten

Wenn Frau Mustera ihren Mitarbeitern die private Nutzung von E-Mails und des Internets in der Arbeitszeit gestattet, sollte sie vereinbaren, welchen Umfang diese Nutzung umfassen darf und dass die Nutzung bestimmte Inhalte nicht betreffen darf. *Das kann sie durch eine Ergänzung des Arbeitsvertrages machen. Sie kann auch eine Betriebsvereinbarung mit ihren vier Mitarbeitern treffen.* Die Erlaubnis kann Frau Mustera mit einer Einwilligung verbinden, dass die Mitarbeiter ihr Kontrollen gestatten, damit weder Inhalt noch Umfang der Nutzung gegen Gesetze und die arbeitsrechtlichen Pflichten verstoßen. Diese Einwilligung muss in Schriftform erfolgen.

V. Datenschutzrechtliche Anforderungen

Miranda Mustera muss ihre Verfahren in einem sogenannten **Verzeichnis für die Verarbeitungstätigkeiten** (früher: Verfahrensverzeichnis) mit folgenden Angaben dokumentieren:

- Name und Kontaktdaten des Verantwortlichen, des Vertreters, ggfs. des gemeinsam Verantwortlichen sowie des etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung
- Rechtsgrundlage
- Kategorie der betroffenen Personen und personenbezogenen Daten
- Kategorie von Empfängern der Daten
- Übermittlung in Drittstaaten
- Löschfristen
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherung

Sie muss ihre **Mitarbeiter auf die Vertraulichkeit von Daten verpflichten** und sie auf den Datenschutz hinweisen bzw. angemessen **schulen** und dies dokumentieren. **Die Geheimhaltungsverpflichtung ist Bestandteil oder Zusatz zum Arbeitsvertrag.** Sie sollte überlegen, wie sie mit einem **Auskunftsersuchen** umgeht, wenn jemand erfahren möchte, welche Daten sie über ihn gespeichert hat.

Sie sollte deshalb am besten schriftlich festlegen, wer außer ihr selbst innerhalb der Belegschaft verantwortlich ist. Sie sollte zusätzlich prüfen, ob sie einen Prozess aufsetzt, falls es zu **Datenverstößen** kommt und sie dies der Aufsicht binnen 72 Stunden (neu) melden muss. Die betroffene Person muss unverzüglich über den Datenverstoß informiert werden.

Frau Mustera muss ein **Löschkonzept** vorsehen *(gesetzlich geregelt für: 6 Jahre Geschäftsbriefe, 10 Jahre steuerrelevante Unterlagen, 6 Monate Bewerbungsunterlagen).* Alle anderen Daten bzw. Dokumente mit personenbezogenen Daten müssen gelöscht bzw. vernichtet werden, wenn sie nicht mehr benötigt werden.
Daran schließt sich die Frage an, wie datenschutzkonform Unterlagen vernichtet werden können und müssen (z. B. Datenträger zerstören, Papierunterlagen mit personenbezogenen Daten schreddern).

VI. Technisch-organisatorische Maßnahmen

Sie betreffen die Frage, wie sicher die personenbezogenen Daten sind *(IT, Sicherheit im Büro/Geschäft);* auch dies muss dokumentiert werden. Miranda Mustera muss insbesondere mit ihrem Steuerberater klären, wie die sensiblen Daten ihrer Mitarbeiter *(Gesundheitsdaten, Religionszugehörigkeit)* gut geschützt sind. Hierzu müssen bestimmte Maßnahmen ergriffen werden (Stichwort: Datenschutz-Folgenabschätzung). Eine Übermittlung per E Mail ohne weitere Sicherheitsmaßnahmen ist datenschutzrechtlich nicht zulässig. Nachstehende Punkte geben einen groben Anhaltspunkt für solche Maßnahmen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren: *Kunden haben keinen Zutritt zu Büroräumen*

b) Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können: *EDV-System wird nach Arbeitsende so gesperrt, dass z.B. Reinigungskraft keinen Zugriff hat.*

c) Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

d) Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

b) Eingabekontrolle/Verarbeitungskontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

c) Dokumentationskontrolle
Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

d) Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

3. Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

4. Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)
Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

Frau Mustera muss ihre Daten so sichern, dass sie sie bei einem eventuellen Verlust wiederherstellen kann.

Weitere Informationen finden Sie unter:

https://www.lfd.niedersachsen.de/startseite/dsgvo/fragen_zur_vorbereitung_auf_dsgvo/
- spezieller Fragebogen der Landesbeauftragten für den Datenschutz Niedersachsen

www.gdd.de
- Gesellschaft für Datenschutz und Datensicherheit mit Mustern (z. B. ADV-Vertrag)

https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html
- Kurzpapiere der Datenschutzkonferenz zu bestimmten Aspekten der DSGVO

Wir danken der AG Datenschutz, DIHK, für die Erarbeitung und Bereitstellung der Informationen.